



UCL

DEVELOPING AN INTERVENTION TO PROTECT OLDER ADULTS FROM CYBERCRIME

Benjamin Havers

Dawes Centre for Future Crime

Department of Security and Crime Science

Faculty of Engineering

University College London

Thesis submitted for the degree of Doctor of Philosophy, 27 March 2025

Primary Supervisor:

Professor Claudia Cooper (CC)

Centre for Psychiatry and Mental Health, Queen Mary University of London
and Division of Psychiatry, UCL

Secondary Supervisors:

Dr Kartikeya Tripathi (KT)

Department of Security and Crime Science, University College London

Dr Alexandra Burton (AB)

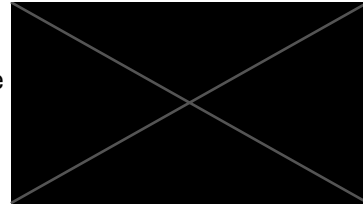
Centre for Psychiatry and Mental Health, Queen Mary University of London
and Department of Behavioural Science and Health, University College
London

Declaration

I, Benjamin Havers, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Date: 27 March 2025

Signature



Acknowledgements

This PhD would not have been possible without the support and encouragement of numerous people along the way. I would like to express my gratitude to all those who have contributed in any form to this thesis and my research.

First and foremost, I am extremely grateful to all my supervisors for their guidance, patience, support and kindness throughout the course of my PhD. In particular, I would like to thank Claudia for her incredible drive and direction, Alex for her unwavering positivity, and Kartikeya for his good humour and willingness to introduce me to a range of useful contacts.

I would also like to extend my sincere thanks to the Dawes Trust, University College London, and the Dawes Centre for Future Crime at UCL for their financial support and resources, making this PhD a possibility.

I want to express my gratitude to Professor Sally McManus (City, University of London) and Dr Wendy Martin (Brunel University of London) for their important contributions to my work as well as their general eagerness to support wherever possible. And to Dr Aiden Sidebottom (University College London), for backing me throughout my time at UCL, during both my master's and PhD.

I am thankful to my friends and family for their support, understanding and encouragement throughout this journey. To my mum and dad, thank you for fuelling my studies with delicious food and drink whenever I visited home. To Katie, thank you for always being there, motivating me to push this through to the end.

UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s)

For a research manuscript that has already been published:

(a) What is the title of the manuscript?

Article 1: Cybercrime victimisation among older adults: A probability sample survey in England and Wales

Article 2: Exploring the factors preventing older adults from reporting cybercrime and seeking help: A qualitative, semistructured interview study

(b) Please include a link to or doi for the work:

Article 1: <https://doi.org/10.1371/journal.pone.0314380>

Article 2: <https://doi.org/10.1155/2024/1314265>

(c) Where was the work published?

Both online

(d) Who published the work?

Article 1: PLOS One

Article 2: Health & Social Care in the Community

(e) When was the work published?

Article 1: 18/12/2024

Article 2: 23/10/2024

(f) List the manuscript's authors in the order they appear on the publication:

Article 1: Benjamin Havers, Kartikeya Tripathi, Alexandra Burton, Sally McManus, Claudia Cooper

Article 2: Benjamin Havers, Kartikeya Tripathi, Alexandra Burton, Wendy Martin, Claudia Cooper

(g) Was the work peer reviewed?

Yes

(h) Have you retained the copyright?

Yes

(i) Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)?

Yes:

Article 1: <https://doi.org/10.21428/cb6ab371.46d2b268>

Article 2: <https://doi.org/10.21428/cb6ab371.8c4e3181>

For multi-authored work, please give a statement of contribution covering all authors

Article 1: Benjamin Havers planned the study and did the data curation, formal analysis, project administration, writing, reviewing and editing. All other others contributed equally in supervision, reviewing and editing.

Article 2: Benjamin Havers planned the study, collected, transcribed and analysed the data and wrote the study. Kartikeya Tripathi, Alexandra Burton and Claudia Cooper contributed to the planning of the study, provided secondary analysis of the data and revised the manuscript. Wendy Martin provided ageing and digital and qualitative expertise and revised the manuscript.

In which chapter(s) of your thesis can this material be found?

Article 1: Chapter 3; Article 2: Chapter 4

e-Signatures confirming that the information above is accurate:

Candidate: *Benjamin Havers*

Date: 27 March 2025

Supervisor: *Professor Claudia Cooper*

Date: 27 March 2025

Table of Contents

Declaration.....	1
Acknowledgements	2
UCL Research Paper Declaration Form: referencing the doctoral candidate's own published work(s).....	3
Abstract	9
Impact Statement.....	11
Who will benefit from this work?.....	11
The public	11
Health and social care, the Fraud Justice Network and the third sector	11
The academic community	12
Government	12
List of Tables	13
List of Figures	13
Abbreviations	14
Chapter 1: Introduction.....	15
1.1 Background.....	15
1.2 Crime and victimisation	16
1.2.1 Crime Science.....	16
1.2.2 Criminology.....	20
1.2.3 Victimisation and Victimhood	24
1.3 Cybercrime.....	30
1.3.1 Terminology	30
1.3.2 Categorisations and typologies of cybercrime	31
1.3.3 Types of cybercrimes	32
1.3.4 Factors associated with cybercrime	35
1.3.5 Impact of cybercrime on businesses	39
1.3.6 Impact of cybercrime on individuals	39
1.3.7 Procedures for reporting cybercrime	41
1.3.8 Cybercrime reporting decision making.....	43
1.3.9 Cybercrime prevention and protection	43
1.3.10 Cybercrime offenders	47
1.4 Ageing	48
1.4.1 Sociological theories of ageing	48
1.4.2 Healthy and successful ageing.....	52
1.4.3 Wellbeing and illness in older age	53
1.4.4 Technology, internet use and aging	55
1.5 Crime and cybercrime against older adults.....	57
1.5.1 Victimisation risk factors among older adults	58
1.5.2 The impact of cybercrime on older adults.....	60
1.6 Summary	61

Chapter 2: Structure and aims of the thesis	62
2.1 Structure of thesis	62
2.1.1 Study 1: Cybercrime victimisation among older adults: a probability sample survey in England and Wales	62
2.1.2 Study 2: Exploring the factors preventing older adults from reporting cybercrime and seeking help: a qualitative, semi-structured interview study	62
2.1.3 Study 3: Stakeholder workshops to generate intervention proposals for increased cybercrime reporting among older adults	63
Chapter 3: Cybercrime victimisation among older adults: a probability sample survey in England and Wales	64
3.1 Introduction	64
3.2 Materials and methods	65
3.2.1 Participants and procedures	65
3.2.2 Measures	66
3.2.3 Analysis	67
3.3 Results	69
3.3.1 Sample description	69
3.3.2 Findings	69
3.4 Discussion	71
3.4.1 Limitations	74
3.4.2 Conclusion	75
Chapter 4: Exploring the factors preventing older adults from reporting cybercrime and seeking help: a qualitative, semi-structured interview study	76
4.1 Introduction	76
4.2 Materials and Methods	77
4.2.1 Participants and procedures	77
4.2.2 Analysis	81
4.3 Results	82
4.3.1 Sample Description	82
4.3.2 Findings	84
4.4 Discussion	104
4.4.1 Barriers to reporting and the value of social interaction	104
4.4.2 Ageism and underreporting	105
4.4.3 Limitations	106
4.4.4 Conclusion	107
Chapter 5: Stakeholder workshops to generate intervention proposals for increased cybercrime reporting among older adults	108
5.1 Introduction	108
5.2 Aims and objectives	109
5.3 Methods	110
5.3.1 Participants	110
5.3.2 Procedures	111
5.3.3 Analysis	113

5.4	Results	114
5.4.1	Holding interactive cybersecurity sessions that bring older adults together	116
5.4.2	Engaging previous victims of cybercrime to offer support and advice to older adults	120
5.4.3	Engaging younger demographics and other trusted individuals in educational and supporting roles	122
5.4.4	Communicating messages that normalise and decatastrophise victimisation	123
5.4.5	Training stakeholders on communicating empathetically and recognising victimisation signs	129
5.5	Discussion	132
5.5.1	Summary of main findings	132
5.5.2	Implications of findings	134
5.5.3	Limitations	136
5.5.4	Conclusions	138
 Chapter 6: Developing an intervention to protect older adults from cybercrime: Online Porcupine		
		139
6.1	Why the Name?	139
6.2	How does it aim to protect older adults from cybercrime?	139
6.3	How does it work?	140
6.4	How does Online Porcupine draw on my consultation findings and previous research?	141
6.4.1	‘Holding interactive cybersecurity sessions that bring older adults together’	142
6.4.2	‘Engaging previous victims of cybercrime to offer support and advice in different contexts’	144
6.4.3	‘Engaging younger demographics and other trusted individuals in educational and supporting roles’	144
6.4.4	‘Communicating messages that normalise and decatastrophise victimisation’	145
6.4.5	Training stakeholders on communicating empathetically and recognising victimisation signs	147
6.5	Other considerations	147
6.6	Scaling up Online Porcupine	148
6.7	Example Online Porcupine Session Structure.....	150
 Chapter 7: Discussion		
		151
7.1	Summary of findings.....	151
7.2	Interpretation of findings	154
7.3	Strengths and Weaknesses	156
7.3.1	Strengths	156
7.3.2	Weaknesses	157
7.4	Implications for policy and practice.....	159
7.4.1	Greater representation of the unique needs and experiences of older adults in the Online Safety Act 2023 Bill	159
7.4.2	Consideration of cybercrime in the Police Race Action Plan.....	160
7.4.3	Incorporation of cybercrime and fraud victimisation information into guidance and/or training for health and social care professionals.....	161
7.4.4	Practical recommendations for increasing cybercrime reporting among older adults	161
7.5	Future research	161
7.5.1	Expanding data collection methods	162

7.5.2	Engaging with ex-offenders	162
7.5.3	Reaching under-served groups.....	162
7.6	Conclusions.....	163
References.....		165
Appendices.....		210
Appendix 1: Study 1 participant information sheet (friends and family)		210
Appendix 2: Study 2 participant information sheet (professionals)		213
Appendix 3: Study 2 participant information sheet (older adults)		217
Appendix 4: Study 2 topic guide (friends and family)		221
Appendix 5: Study 2 topic guide (older adults)		223
Appendix 6: Study 2 topic guide (professionals)		225
Appendix 7: Study 2 consent form		227
Appendix 8: Study 2 participant demographic questionnaire (friends & family).....		229
Appendix 9: Study 2 participant demographic questionnaire – older adults		231
Appendix 10: Study 2 participant demographic questionnaire – professionals.....		233
Appendix 11: Study 2 infographic (older adults)		235
Appendix 12: Study 2 infographic (family, friends and health and social care professionals) ...		236
Appendix 13: Study 2 physical flyer.....		237
Appendix 14: Study 2 ethics approval		238
Appendix 15: Study 3 social media publicity		239
Appendix 16: Study 3 consent form.....		240
Appendix 17: Study 3 participant information sheet.....		242
Appendix 18: Study 3 direct solicitation message		245
Appendix 19: Study 3 workshop agenda.....		246
Appendix 20: Study 3 framework matrix		247
Appendix 21: Study 3 ethics approval		254
Author contribution statement		255

Abstract

Background:

As older people spend more time online with digitalisation, they may, due to risk factors including social isolation and poor health, be disproportionally susceptible to cybercrime. I aimed to explore how risk factors vary between age groups, and how older age groups experience cybercrime, to inform the design of protective resources.

Methods:

Study 1: I conducted logistic regression analysis of responses from the 2019/20 Crime Survey for England and Wales, investigating risk of cybercrime victimisation and financial loss across age groups and other socio-economic characteristics. Study 2: I interviewed victims aged 60+, their family and stakeholders to explore cybercrime reporting decisions; conducting a reflexive thematic analysis. Study 3: I held stakeholder workshops to develop approaches to increase cybercrime reporting; conducting a framework analysis.

Results:

Study 1: Those reporting poor health (OR 1.74, $p=0.001$), were at greater risk of cybercrime victimisation. Despite being less likely to report any cybercrime in the past year, people aged 75+ were more likely to report financial loss from cybercrime (OR 4.25, $p=0.037$) and repeat cybercrime victimisation (OR 2.03, $p=0.074$). Study 2: I identified four themes around reporting experiences including the value of social support. Study 3: I developed five overarching intervention proposals for supporting older adults to avoid or report victimisation, including communications that normalise and decatastrophise cybercrime.

Conclusion:

While younger adults are more at risk from cybercrime, older adults reported more severe offences (repeat victimisation and associated financial loss), indicating they may be more reluctant to report less serious offences. This reluctance may stem from shame, past

experiences of unhelpful responses, and lack of awareness. Social support from peers and professionals can aid reporting and recovery. Stakeholders proposed strategies, including around training and communications, to increase reporting. These discussions informed 'Online Porcupine', a resource for local community organisations to hold interactive cybersecurity sessions.

Impact Statement

Who will benefit from this work?

The public

This work is published in open access, peer-reviewed journals, PLOS One (Havers, Tripathi, Burton, McManus, et al., 2024a) and Health and Social Care in the Community (Havers, Tripathi, Burton, Martin, et al., 2024b). The PLOS One article was selected by the journal for a press release, and featured in at least 14 news stories from 12 international news outlets, from the United States to New Zealand, including Microsoft's MSN (Beech, 2024). It was also covered in German language articles by Swiss (Von Kempkens, 2024) and German (Reckert, 2024) news outlets.

Several research participants described benefiting from sharing their cybercrime victimisation, feeling heard, and discussing how to keep safe online. One remarked that “you're the first one who has made even an attempt at understanding it”.

My findings present avenues for designing interventions that protect older adults from cybercrime, including informing the development of my Online Porcupine intervention proposal.

Health and social care, the Fraud Justice Network and the third sector

This thesis includes recommendations that police officers and staff, employees of Action Fraud or its imminent replacement organisation, and employees of financial institutions can add to their toolkit for effectively and appropriately attending to older adults and older victims of cybercrime. To disseminate some of my initial findings to these audiences, I wrote a chapter on cybercrime against older adults for a guidebook for specialist and new police officers, entitled ‘Policing Public Protection: A Companion Guide’ (Aplin et al., 2024), edited by former police detective Dr Rachael Aplin (Leeds Beckett University).

The academic community

Though only recently released, my preprints (Havers, Tripathi, Burton, Martin, et al., 2024a; Havers, Tripathi, Burton, McManus, et al., 2024b) and aforementioned published papers have been recognised in a number of peer reviewed scientific articles internationally, such as Cole's (2024) investigation into the consequences of romance scams in the USA, Houtti et al.'s (2024) international scam survey and Azam et al.'s (2024) analysis of a cybersecurity awareness model for older adults in Malaysia. I presented my initial findings at the national British Society of Criminology conference in May 2023, and in June 2023 to UCL's Department of Security and Crime Science prior to upgrading from MPhil to PhD.

Government

I presented my first study, a quantitative analysis of data from the Crime Survey for England and Wales, at the British Society of Criminology Conference in May 2023. A Home Office official from their Crime Analysis Unit requested that I send him the article, as it was an area they were particularly interested in at that time, as they were developing their 'Stop! Think Fraud' campaign. My research is cited in written UK parliamentary evidence, submitted by the Violence, Health, and Society (VISION) consortium funded by the UK Prevention Research Partnership, in relation to ageist stereotyping and discrimination and how intersectionality affects older people and requires distinct policy responses (VISION, 2023).

List of Tables

Table 3.1:	Sociodemographic characteristics of the sample and multivariate associations with cybercrime victimisation and repeat victimisation.
Table 3.2:	Financial loss summary statistics and univariate analysis
Table 4.1:	Sample characteristics for professional stakeholders
Table 4.2:	Sample characteristics for older adults
Table 5.1:	Sociodemographic and role characteristics of workshop participants
Table 5.2:	Activities and activity components identified in workshops in response to the goal and objectives presented
Table 6.1:	Demonstration of how Online Porcupine design maps to consultation findings

List of Figures

Figure 1.1:	Clarke and Eck's Crime Triangle
Figure 1.2:	Crime victimisation by age group for the year ending March 2023
Figure 5.1:	Developing and evaluating complex interventions framework
Figure 5.2:	Workshop theory of change template
Figure 7.1:	Finding, consultation, prototype illustration

Abbreviations

AB	Dr Alexandra Burton
ACAS	Advisory, Conciliation and Arbitration Service
BA	Bachelor of Arts
BBC	British Broadcasting Corporation
BH	Benjamin Havers
CC	Professor Claudia Cooper
CPTED	Crime Prevention through Environmental Design
CSEW	Crime Survey for England and Wales
DoS	Denial of Service
FJN	Fraud Justice Network
GCHQ	Government Communications Head Quarters
GDPR	General Data Protection Requirements
GP	General Practitioner
HMPPS	His Majesty's Prison and Probation Service
ICO	Information Commissioner's Office
ICT	Information Computer Technology
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
KT	Dr Kartikeya Tripathi
LSOA	Lower-Layer Super Output Area
MCI	Mild Cognitive Impairment
MPS	Metropolitan Police Service
MRC	Medical Research Council
MSc	Master of Science
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NFIB	National Fraud Intelligence Bureau
NHS	National Health Service
ONS	Office for National Statistics
OR	Odds Ratio
PhD	Doctor of Philosophy
PPI	Patient and Public Involvement
PTSD	Post-Traumatic Stress Disorder
QMUL	Queen Mary University of London
RCT	Randomised Control Trial
ROCU	Regional Organised Crime Unit
SCP	Situational Crime Prevention
SMS	Short Message Service
U3A	University of the Third Age
UCL	University College London
UK	United Kingdom
USA	United States of America

Chapter 1: Introduction

1.1 Background

Just seven weeks after graduating with a BA in Spanish and Portuguese with Business, I was on the streets of Epsom and Ewell as a neighbourhood police officer, using my language skills to liaise with the large Brazilian and Madeiran communities around the Surrey–London border. The Police Now Graduate Programme was created to bring energetic individuals with fresh ideas into an institution often considered out of touch with societal change. I was quickly tasked with producing innovative, long-term solutions to ‘new’ crimes such as catalytic converter theft, hate incidents and cuckooing (the takeover of a vulnerable person’s home for use as a base for dealing drugs). I developed a keen interest in crime prevention – particularly with regards to vulnerable adults - and with that came a passion for evidence-based and intelligence-led policing. I subsequently joined HM Prison and Probation Service (HMPPS) as a Regional Counter-Terrorism Intelligence Analyst. For 9 months, I monitored and analysed the activity of extremist prisoners across seven London jails, learning from academic research around extremism and de-radicalisation, including the work of the UCL Department of Security and Crime Science, which informs Ministry of Justice and HMPPS policy decisions.

After completing the department’s MSc in Countering Organised Crime and Terrorism, I successfully applied for the UCL / Dawes Centre for Future Crime PhD studentship entitled ‘Developing an Intervention to Protect Older People from Cybercrime’, motivated by my interests in evidence-based crime prevention with human vulnerability and human-factor cybersecurity.

In this thesis, I have conducted quantitative and qualitative research to explore how older people experience, and report, cybercrime to inform resources to support victims. In this chapter, I explain the context of this work - exploring the fields of crime and victimisation, cybercrime,

ageing and finally in the intersection of those topics, what is known about the risks of crime and cybercrime among older people.

1.2 Crime and victimisation

1.2.1 Crime Science

Crime science is, quite simply, the application of science to crime. Its objective is to learn how to reduce it through prevention, disruption, detection and offender management. It is a crime scientist's job to bring together those diverse but relevant perspectives to devise, test and implement interventions to reduce crime (Wortley et al., 2018). There are several principal approaches within Crime Science, that have been applied to cybercrime to lesser or greater extents. In the sections below I outline five fundamental crime science approaches: Crime Prevention through Environmental Design (CPTED), Defensible Space, Situational Crime Prevention, Routine Activities and Crime Pattern Theory, and consider their relevance to my PhD.

1.2.1.1 *Crime Prevention through Environmental Design (CPTED)*

CPTED was first coined by Ray Jeffery (1972) in his book of the same name. It is the planning, design or management of the physical environment, including buildings, streets and parks, with the aim of preventing or reducing crime. Examples include increasing natural surveillance by widening alleyways, or preventing offender access using physical barriers. The proactive and reactive application of the CPTED approach has become a routine practice, for town planners, architects and Neighbourhood Watch committees. Academically, there is a growing evidence base for diverse CPTED techniques for different spaces and crimes, such as antisocial behaviour in town centres (Piroozfar et al., 2019) and residential burglary (Tseloni et al., 2017).

A small number of studies have applied CPTED to cybercrime (which I will define and explore in more depth in 1.3), not by tailoring digital design but rather in the context of altering physical environments to protect physical information technology (IT) infrastructure in organisations (Lim,

2021; Beni et al., 2024; Whitford, 2018). At the time of writing there are no studies which explicitly apply CPTED techniques to cybercrime against members of the public rather than businesses or organisations.

1.2.1.2 *Defensible Space*

Linked to CPTED is Newman's *Defensible Space* theory, which is concerned with altering the physical environment to empower residents to take control of their own surroundings, exercise guardianship, and reduce crime and antisocial behaviour (Newman, 1997). It has primarily been applied to low-income housing estates, and examples include assigning ownership to previously public or shared spaces, such as external hallways (Warwick & Lees, 2022). While concepts of defensible space are more often applied to crime in the 'real world' than in 'cyberspace', it has some applicability to cybercrime. Ehlert & Rüdiger (2020) argue that social media platforms, for instance, can foster ownership and territoriality through page customisation and the facility of online community groups. Mawby (2017) critiques Newman's Defensible Space, suggesting that the theory's focus on territoriality erroneously implies that offenders must be outsiders and cannot be people already living or active within communities. Mawby's point is of course true of online as much as physical communities; the threat can be both internal (e.g. malicious activity by people with authorised access to an organisation's system) and external (e.g. hackers).

1.2.1.3 *Situational crime prevention*

Clarke's Situational Crime Prevention (SCP) views every crime as an interaction between an offender and their situation. SCP involves altering conditions so that the offender, who according to the Rational Choice Perspective (Cornish & Clarke, 2017) is in control of their own decision making, opts against committing a crime on the basis that the risk is greater than the reward (Clarke, 2017). Clarke proposes 25 SCP techniques, which are classified in five categories; (i) Increase the effort, (ii) Increase the risks, (iii) Reduce the rewards, (iv) Reduce provocations, and (v) Remove the excuses. Ho et al. (2022) conducted a systematic literature review of SCP for

cybercrime, and compiled a list of tools and activities that cover the majority of Clarke's 25 techniques. For 'deny benefits', for example, which comes under 'reduce the rewards', Ho et al. (2022) cite multiple studies highlighting data encryption as an effective SCP technique (e.g. Hinduja & Kooi, 2013; Willison & Siponen, 2009). Encryption is the scrambling of sensitive, confidential or personal information into a secret code that online intruders or 'hackers' cannot read when stored or transmitted (Stouffer, 2023).

The most enduring criticism of SCP is, according to Tilley & Sidebottom (2014), that it simply displaces crime from one place to another because it fails to address the underlying root causes of the crime. Bowers & Guerette (2014), however, argue that the degree to which displacement occurs is unlikely to match the degree to which crimes are prevented through SCP, because prospective offenders offend in places they're familiar with, and crime opportunities are not uniformly available. There is currently no research examining whether displacement of cybercrime occurs as a result of altering the situational conditions of the internet or internet users.

1.2.1.4 The Routine Activities Approach

Cohen and Felson's (1979) Routine Activities Approach is the most relevant to this thesis. It contends that crime happens because in the routine activities of day-to-day life, potential offenders and targets cross paths, and that there may be an absence of guardianship over that target. Crime happens when these three elements converge. The target may be a person, product, premises, system or process, such as a computer network. The guardian could be closed circuit television surveillance or a firewall. The potential offender could be automated too, like a computer virus. The Routine Activities Approach can be used to explain, and attempt to alter, the dynamics of individual crime events. Clarke and Eck's Crime Triangle (2003), also known as the problem-solving triangle, is an extension of the Routine Activities Approach.

Figure 1.1: Clarke and Eck's Crime Triangle (Adapted from Felson, 2017)



It comprises an inner and outer layer. The inner layer depicts the three aforementioned core elements. The outer layer shows their respective 'supervisors'; the handler supervises the would-be offender, the manager supervises the crime setting, and the guardian supervises the target. An absence of any of these supervisors increases the likelihood of a crime (Felson, 2017). The crime triangle has been applied in various contexts, from public sector corruption (Porter & Graycar, 2016) to kidnapping for ransom (Pires et al., 2014) and also cybercrime: Junger et al., (2017) for example found that frequency of time spent online is associated with victimisation, and that activities such as online selling, online banking and use of social media are associated with higher risks of certain types of cybercrime such as consumer fraud and online harassment. Yar (2005), however, argues that the convergence of the three components that are essential for crime to occur according to the Routine Activities Approach do not fit cybercrime so neatly. Unlike in physical environments where people, objects and activities are clearly located in spatial

and temporal configurations, Yar (2005:424) proposes that “the cyber-spatial environment is spatio-temporally disorganised”, citing internet use that spans work and leisure time and multiple different time zones, as well as the lack of geographical spatial barriers. He accepts, however, that capable guardians, suitable targets and motivated offenders do exist online, albeit with nuanced characteristics, such as limited target visibility.

1.2.1.5 Crime Pattern Theory

Linked to the Routine Activities Approach is Crime Pattern Theory (Yar, 2005). This proposes that offenders generally commit crime in their areas of familiarity, or ‘awareness spaces’, where they have the greatest knowledge of crime opportunities and detection risks. ‘Hotspots’ occur where awareness spaces and crime facilitators intersect, e.g. busy areas and places with limited guardianship. Advances in computing have led to the creation of a new strand of crime science, geo-spatial analysis and crime mapping, an effective and innovative way of conveying otherwise complex crime patterns, including hotspots, to practitioners in a useful but visually appealing way (Johnson, 2017). Though cybercriminals have been mapped geographically in terms of what country they are from (e.g. Lusthaus et al., 2020) Crime Pattern Theory has yet to be applied explicitly to digital spaces, though it is plausible that awareness spaces and high-traffic areas exist in the form of websites as much as they exist in the physical world.

1.2.2 Criminology

Whereas crime science revolves around evidence-based practices and the use of data analytics to inform policy and practice around crime prevention (Chan & Bennett Moses, 2016), criminology examines crime as a social phenomenon, often focusing on the complexities of criminal behaviour, social structures, and the interplay between individual actions and societal norms (Hawks Jr & McDonald-Lopez, 2021). Whilst crime science focuses on how to stop or prevent crime, criminology explores why crime happens and why offenders offend (Wortley et al., 2018). This thesis focuses on the victim experience and hence criminology is less relevant

than crime science. However, in order to build a picture of crime and all its elements and core theories, I describe three of the most prominent criminological perspectives below.

1.2.2.1 Classical

The classical school of criminology, which originates in the 18th century work of Beccaria (1764) and Bentham (1781), is grounded in the principles of rationality and utilitarianism. Proponents contend that individuals are rational actors who make decisions based on a cost-benefit analysis, seeking to maximise pleasure and minimise pain. Rational choice theory, or perspective, has foundations in the classical framework. It views criminal behaviour as the result of normal criminal motivations, desires and preferences. “At its core are the concepts of choice and decision-making and the centrality of the crime event to continued criminal activity: that success in committing crimes drives the development of criminal lifestyles, while failure leads to reduction in offending or even to desistance” (Cornish & Clarke, 2017:29).

The rational choice perspective has been widely applied to research on crime and crime prevention. Alonso Berbotto & Chainey (2021), for example, investigated the decision making processes of oil thieves in Mexico, whilst Beauregard et al. (2011) used a rational choice theory approach to describe the ‘hunting’ process of serial sex offenders in Canada. Some critics find the cost-benefit analysis component of this theory oversimplistic, as it does not account for the emotional, social, psychological and cognitive factors that may influence rationale (Ward et al., 2006).

1.2.2.2 Positivism

Positivism in criminology emerged in the 19th century as a reaction to the classical school. It suggests people commit crime in response to internal or external influences (The Chicago School, 2021). Indeed, in the context of cybercrime, Palmieri et al. (2021) observed that there is

a positive association between likeliness to engage in cybercrime and both impulsivity (spontaneity of behaviour) and reward reactivity (sensitivity to gains).

Biological positivism asserts that criminality is determined by biological factors including genetic and hormonal influences. This perspective has been discredited for its links to discrimination and eugenics, particularly in the context of identifying ‘born criminals’ and reinforcing social inequalities and marginalisations (Shichor, 2014). Nevertheless, a small number of studies, such as that of Liao et al. (2004) and Toshchakova et al. (2018), have found that chemical imbalances are associated with aggressive and criminal behaviour.

1.2.2.3 Sociological

Sociological approaches to criminology suggest that crime is shaped by factors which are external to the individual, including their peer group and their family (SCCJR, 2016). Social Learning theory, developed by Bandura & Walters (1963), proposes that individuals learn behaviours, including criminal ones, through observation and imitation of others, particularly within their social environment. This position is supported by Haynie & Osgood (2005), whose examination of the contribution of peer relations to delinquency revealed that “adolescents engage in higher rates of delinquency if they have highly delinquent friends and if they spend a great deal of time in unstructured socializing with friends” (p.1109).

Labelling theory contends that the labels the authorities, or society, assign to individuals, influences their self-identity and behaviour (Thompson, 2016). According to the theory, labelling “has the unintended consequence of amplifying the very phenomenon that it is intended to suppress, by virtue of the self-fulfilling prophecy that it engenders” (Fine, 1977). Though Labelling theory has little empirical validation, studies by Restivo & Lanier (2015) and Bernburg & Krohn (2003) found that official intervention (e.g. arrest) by the authorities is associated with increased delinquent self-identity and future offending.

General Strain theory (Agnew, 1992) proposes that there are three major types of strain that can lead to criminality as a coping mechanism. The first is a failure to achieve positively valued goals, referring to the strain experienced when individuals are unable to attain culturally approved goals such as educational achievements or financial success. The second is the removal of positively valued stimuli, which relates to the loss of something valued, such as a job or family member. The third is the presentation of negatively valued stimuli, which occurs when an individual is exposed to negative experiences such as neglect, abuse or victimisation. This theory is commonly applied to different crime phenomena today, from investigations into the effects of military combat experience on mental health and subsequent antisocial behaviour (Watts & Wright, 2021), to bullying victimisation as a precipitator of involvement in delinquency (Glassner, 2020).

Subcultural or subculture theory, first introduced by Cohen (1955), examines how certain groups or subcultures within society develop their own norms, values, and behaviours, which may deviate from, or conflict with, mainstream societal standards. Subculture theory helps explain why individuals in these groups may engage in criminal or deviant behaviour to conform to norms of their subculture (Stancu, 2021). Subculture theory has been applied to the study of gangs (e.g. Fader & León, 2024), where members adopt a distinct set of values that prioritise loyalty, aggression and criminal activity. It has been extended to online communities, such as the Incel (Involuntary Celibate) movement. Members of this subculture may develop shared beliefs and norms that justify their feelings of resentment and hostility towards women, leading to violent and sexual offending (O'Malley et al., 2022).

Finally, Shaw & McKay's (1942) Social Disorganisation theory contends that disorganised neighbourhoods are not capable of controlling their younger members, who are free to follow their 'natural inclinations'. A key tenet of this theory is that communities exist on a spectrum of organisation, and that socially organised communities have solidarity, cohesion and integration

which are collectively conducive to lower crime rates. Contrastingly, disorganised communities lack the rules and interventions that would otherwise maintain order (Kubrin, 2009). In its most basic form, this perspective generalises, demonises and places blame on people living in lower socioeconomic urban areas. However, contemporary applications of the theory, such as Errol et al.'s (2021) examination of the influence of changing family structures on crime, look at specific factors that might cause disorganisation. They found that increased divorce and out-of-wedlock birth rates (a proxy for family structure) is a significantly positive determinant of property crime and violent crime, and overall criminal activity is promoted by urbanisation (a proxy for community structure) – the increasing share of a population living in urban areas which “brings about high rates of residential mobility, which disrupts the ability to establish and maintain social ties” (p. 521).

1.2.3 Victimisation and Victimhood

In this thesis I refer to ‘victims’, ‘victimisation’ and ‘victimhood’. Under the UK Victim’s Code, a victim of crime is “a person who has suffered harm, including physical, mental or emotional harm or economic loss which was directly caused by a criminal offence” or “a close relative of a person whose death was directly caused by a criminal offence” (Code of Practice for Victims of Crime in England and Wales, 2020:3). Victimisation, whilst commonly used to describe the unfavourable treatment of someone in the workplace (ACAS, 2024), is used in this thesis to describe the becoming, or making of, a victim of crime (Collins English Dictionary, 2024). Victimhood is the state of being a victim (Collins English Dictionary, 2025).

Victim ‘vulnerability’ is unique to each individual and their experiences, so is difficult to conceptualise (Fineman, 2010; Wrigley & Dawson, 2016). Vulnerability can manifest pre-crime, in that a vulnerable person is less able to protect themselves from exploitation (or any form of victimisation) due to their possession of particular characteristics (HMICFRS, 2023). Vulnerability in this sense is akin to susceptibility. Vulnerability can also manifest post-

victimisation, when an individual's particular characteristics, such as age, illness, disability or isolation, increase the likelihood of harm (Sentencing Council, 2025).

Here, I will outline some of the key concepts and theories relating to victims and vulnerability.

1.2.3.1 Repeat Victimisation

Repeat victimisation is where an individual experiences crime victimisation more than once over a period of time (Farrell & Pease, 2017). There are three important principles around repeat victimisation that can be useful when considering crime prevention:

First, victims of crime experience a higher risk of future victimisation in the wake of an initial victimisation. Second, this elevated risk has a time-decay; it is highest immediately after a victimisation and falls over time. Combined, these two findings suggest that previous victims have a higher risk of future victimisation, but this risk decays over time, in the order of a few weeks or months. To prevent repeat crimes, in other words, resources should be deployed immediately after a crime if we hope to prevent its recurrence. The third observation is that RV is concentrated among a very small number of individuals. This means that focusing on only previously victimised individuals will result in more efficient use of prevention resources per unit than if the entire population were targeted (Farrell & Pease, 2017:28).

This phenomenon is well-documented in criminological and crime science literature and encompasses various forms of victimisation, including but not limited to financial fraud (J. A. Snyder & Golladay, 2024) and vandalism (Suzuki et al., 2024).

1.2.3.2 Victim Precipitation theory

Victim Precipitation theory proposes that victims contribute to the criminal event that has harmed them, either through facilitation or provocation. Victim facilitation refers to situations where the victim inadvertently creates opportunities for the crime to occur, such as leaving doors

unlocked or displaying valuables in public, whereas victim provocation involves actions by the victim that may incite the perpetrator's aggression, such as verbal confrontations or aggressive behaviour (Lasky, 2019). Critics of victim precipitation theory argue that it leads to victim-blaming attitudes that diminish the responsibility of perpetrators (Cortina et al., 2018). Nevertheless, studies such as Cross's (2019) exploration into accountability in fraud victimisation show that professionals who deal with victims of crime are indeed often willing to place blame on victims who lack sufficient caution.

1.2.3.3 Shattered Assumptions

Shattered Assumptions theory posits that victimisation can “strike at the core of our inner world”, shattering our fundamental assumptions that the world is benevolent and meaningful and that ‘the self is worthy’ (Janoff-Bulman, 1999), causing significant psychological, physical, behavioural and social consequences for the victim. In other words, victimisation can cause assumptions about the world being a predominantly good place with good, caring people and where outcomes are fair and deserved, to break down. Likewise, our assumptions about ourselves being competent, decent and engaged in positive behaviours are ruined (ibid). Shattered Assumptions theory can be relevant to cybercrime and for developing interventions that rebuild those assumptions. In the first study to apply this theory to cybercrime, Borwell et al.'s (2022) Dutch survey found that the anonymity and remoteness of cyber offences still resulted in the victim's sense of security being impacted to the same magnitude as those experiencing traditional offences. Additionally, victims who received loss compensation experienced a lower impact on their emotional well-being than victims who did not, which corresponds with the theory's premise that shattered assumptions around, for example, fairness and deservedness can be restored.

1.2.3.4 *Secondary Victimisation and Learned Helplessness*

Secondary Victimisation is when the victim of a crime suffers further negative consequences and harm, from their contact with societal institutions such as law enforcement and the criminal justice system (Pemberton & Mulder, 2023). Unfavourable aspects of this contact might include exposure to the offender, interrogation about their experience, and inappropriate or insensitive comments by officials (European Institute for Gender Equality, 2024). Evidence of this phenomenon has been found across several different crime types, from domestic violence survivors navigating scepticism and pressure in the family law system (Laing, 2017) to victims of road traffic collisions distressed by compensation procedures (Cotti et al., 2004).

Individuals who have experienced repeated victimisation despite initial attempts at seeking justice may come to believe that their actions will not change their situation, leading to a state of learned helplessness. Learned Helplessness, first proposed by Maier & Seligman (1976), refers in the context of crime to “the emotional numbing and maladaptive passivity sometimes following victimization. Victims may learn during the victimisation episode that responding is futile” (Peterson & Seligman, 1983:103), and that they have little or no control over their circumstances. In cases of domestic violence or sexual assault, victims may feel trapped and unable to escape their circumstances (Livingston et al., 2007). Learned helplessness has also been linked to online abuse and bullying through social media; whereby offender anonymity encourages group offending, causing victim depression and helplessness (Prihadi et al., 2019).

Though it emphasises the intense feelings of vulnerability and despair that can be experienced by victims of abuse, learned helplessness theory is arguably disempowering and victim-blaming as it fails to acknowledge victims’ resilience, for example cultivated by mindfulness and redemptive storytelling, discussed below.

1.2.3.5 *Trauma and resilience*

Trauma is “any disturbing experience that results in significant fear, helplessness, dissociation, confusion, or other disruptive feelings intense enough to have a long-lasting negative effect on a person’s attitudes, behavior, and other aspects of functioning” (APA, 2025). Post-Traumatic Stress Disorder (PTSD) is a psychiatric disorder whereby such symptoms last for a prolonged period after the traumatic event and start to interfere with aspects of daily life, such as relationships and work. People with PTSD may continue to feel stressed or frightened, despite not being in danger (NIMH, 2024). Crime victimisation can result in trauma and PTSD. Satchell et al.'s (2023) systematic review of psychological consequences of crime in older victims, for example, identified 30 different psychological symptoms, including sleep disorder, self-blame, depression, anxiety and panic attacks. Crimes ranged from theft and pension fraud to rape, assault and criminal damage. In treating traumatised victims of crime, the authors advocate use of the Impact of Event Scale (Horowitz et al., 1979), a score-based system for assessing the severity of distress associated with a specific traumatic event in order that individuals in need of extra and specific support can be identified.

Resilience is “the process of adapting well in the face of adversity, trauma, tragedy, threats, or significant sources of stress—such as family and relationship problems, serious health problems, or workplace and financial stressors” (APA, 2020). Thompson et al. (2011) found that mindfulness and acceptance are associated with greater adjustment following trauma, thus recommending more psychological interventions based around mindfulness and acceptance for those experiencing PTSD. Mindfulness, a technique rooted in Buddhism and meditation, consists of “self-regulation of attention so that it is maintained on immediate experience, thereby allowing for increased recognition of mental events in the present moment” and “adopting a particular orientation toward one’s experiences in the present moment, an orientation that is characterized by curiosity, openness, and acceptance” (Bishop et al., 2004:232). Acceptance,

which can be facilitated by mindfulness, is made up of three parts: the observation of psychological events; letting go of the desire to alter the form or frequency of these events; and differentiating actual events from the psychological experiences that are evoked by outside events (Follette et al., 2004). Mindfulness as a strategy for adjusting to trauma caused by crime victimisation must be considered with caution. An emphasis on acceptance and ‘letting go’ in the crime victimisation context could imply that fault lies with the victim rather than the offender (Reyes, 2024).

Whilst mindfulness and acceptance are primarily internal cognitive processes, Delker et al. (2020) discuss the power of ‘redemptive storytelling’ of trauma – the sharing of stories of trauma and self-identification as a survivor to a public audience. They note that victimisation often entails the loss of agency, control and choice, and that speaking out about traumatic experiences represents a form of resistance against societal stigma that can be empowering and self-healing. They discuss public speakers’ other-empowering ‘advocacy’ role, acting on behalf of other survivors to challenge injustices and support social action. Delker et al. (2020) cite successful advocacy initiatives among victims of rape and intimate partner violence (IPV), in which victims-turned-activists have fostered community self-empowerment and healing through peer-to-peer redemptive storytelling (Schultz et al., 2016; White, 2001).

1.2.3.6 Intersectionality & victimisation

A more recent approach to victimology centres around how social and sociodemographic contexts, including age, gender, class and ethnic and other minoritised status, can shape victim experience. Intersectionality is a critical framework used to examine how systematic inequalities exacerbate the specific experiences of individuals belonging to more than one marginalised group, and to explore how these inequalities might be addressed (Cho et al., 2013). Zaykowski et al. (2019), for instance, used an intersectional approach to examine how the likelihood of victims reporting a crime to the police is influenced by gender, ethnicity and socioeconomic status.

Zaykowski et al. found that among women, sociodemographic disadvantage was associated with a greater likelihood of reporting crime, with women experiencing socioeconomic disadvantage and low educational attainment the most likely to report. They postulated that fewer help-seeking options, stemming from deep-rooted race and class oppression might explain this finding. Macdonald et al. (2023) examined experiences of racist or homophobic hate crimes against individuals with a disability or mental health condition in the northeast of England. They found that many people with intersectional identities were not taken seriously or believed by the authorities due to their learning disability or mental health issue. They recommend greater recognition of intersectionality by the authorities, and a more coordinated multi-agency response that considers the multiple and complex needs of intersectional victims and survivors.

1.3 Cybercrime

1.3.1 Terminology

Cybercrime is the subject of an extensive body of terminology that is evolving as technology advances, including an array of prefixes and suffixes that are often used arbitrarily among professionals and day-to-day users. The term ‘cybercrimes’ is used synonymously with ‘cyber crime’ (with a space), ‘digital crime’ and ‘online crime’. The prefix ‘cyber’ can be applied to almost any offence or phenomenon that is facilitated by the internet or a digital device, for example ‘cyberbullying’ and ‘cyberfraud’. There are also multiple terms for the criminals who commit fraud and/or operate online, including fraudster, scammer, scam artist, con artist, threat actor and malicious actor - each with different nuance. In this thesis, I will use the term ‘cybercrime’, as is standard in UK law enforcement and criminal justice system (CPS, 2018), and ‘offender’ and ‘potential offender’ to describe, respectively, persons who have committed or are *motivated* to commit a crime as is standard in crime science (Wortley et al., 2018). I will also refer to ‘fraud’ and ‘scams’. The UK legal definition of fraud is “the act of gaining a dishonest advantage, often financial, over another person” (CPS, 2022a). The definition of ‘scam’, often

described as a type of fraud (e.g. DeNicola, 2024), is “to trick someone into giving you money or giving you some advantage, in a dishonest and often illegal way” (Cambridge Dictionary, 2024), thus the distinction is that scams involve an element of trickery. Where I introduce other types of fraud and scams in this thesis, I will define them.

1.3.2 Categorisations and typologies of cybercrime

Clarifying the boundaries and essential features of an offence or category of crime allows us to measure, understand, and respond to it effectively. It circumscribes estimates regarding its extent, the legality or morality of activities, and enables concepts to be accurately communicated in criminological theory and research, and intervention and preventive strategies (Payne, 2020). There is no clear consensus on the definition of cybercrime. Phillips et al. (2022), who reviewed cybercrime definitions, typologies and taxonomies, conclude that:

There is no single clear, precise and universally accepted definition of cybercrime a fact that is acknowledged by both academics and organizations alike, [and that] the articles in this review did not identify a jurisdiction in the world that has a specific single offence of ‘cybercrime’ (Phillips et al., 2022:382).

The European Commission, defines cybercrime as “criminal acts committed using electronic communications networks and information systems or against such networks and systems” (European Commission, 2007).

Cybercrime is becoming industrialised; driven by data analytics and sometimes involving state-level collaboration (Stryker & Kavlakoglu, 2024). Wall's (2007) definitions account for these innovations and complexities:

Cybercrimes are criminal or harmful activities that are informational, global and networked and are to be distinguished from crimes that simply use computers. They are the product of networked technologies that have transformed the division of criminal

labor to provide entirely new opportunities and new forms of crime which typically involve the acquisition or manipulation of information and its value across global networks for gain (Wall, 2007:4).

Wall (2007) proposes a three-category classification system consisting of: ‘crimes against the machine’ such as hacking (“the use of illicit means to gain unauthorized access to a digital device, computer system or computer network” (Kosinski, 2024:)); ‘crimes using the machine’ which are computer-assisted offences, such as online fraud; and ‘crimes in the machine’ including online hate crime (“hostility based on race, religion, disability, sexual orientation or transgender identity” (CPS, 2022b)) and other content-based crimes. This system informed The European Commission’s approach to classifying cybercrime (Helmbrecht, 2016), whose typology consists of ‘offences unique to computers and information systems’, ‘traditional offences’ and ‘content-related offences’.

In a dichotomous approach, first introduced by Brenner (2007), cybercrime offences are categorised as cyber-dependent and cyber-enabled. Cyber-dependent crimes require the use of digital technology, whilst cyber-enabled crimes are traditional crimes that are facilitated or made easier using digital technology.

1.3.3 Types of cybercrimes

Cybercrime is becoming increasingly sophisticated, with criminal innovations that mirror legitimate, artificial intelligence-led technological developments. Artificial intelligence is “technology that enables computers and machines to simulate human learning, comprehension, problem solving, decision making, creativity and autonomy” (Stryker & Kavlakoglu, 2024).

Most high profile scams are examples of ‘Authorised Push Payment’ (APP) Fraud, where the victim is persuaded, under false pretences, to transfer funds from their bank account to a fraudster’s account. Typically, the victim will be persuaded that the fraudster is a legitimate

payee – often an authority or trusted relation. In so-called grandparent scams, fraudsters pose as a grandchild or family member in distress, saying they have been arrested or have a medical emergency, and requesting urgent financial assistance. Contact is usually via SMS or messaging applications, and may read like the following:

Hi Grandad, I've been robbed on holiday and all of my bank cards have been stolen. So sorry to ask but please could you send some money to my friend's account? They will then withdraw it for me so that I have some cash xx

There are fears that scammers have begun to use artificial intelligence (AI) and voice cloning to conduct such scams via phone call, though this is not yet widespread.

1.3.3.1 Romance Scams

Romance scams involve fraudsters establishing non-legitimate romantic relationships with individuals online who are seeking companionship or friendship. The scammer builds trust and emotional connection with the victim before fabricating a crisis or financial need, prompting the victim to send money or provide personal information. Older adults, who are particularly at risk of loneliness and isolation, are vulnerable to these scams, which can result in significant financial losses and emotional distress (Bailey et al., 2021). Previously, suspecting victims have been able to complete a reverse image search to establish whether their love interest's profile picture is genuinely theirs (though this is not a commonly known technique of investigation, and requires a level of technological skill). AI is complicating matters by creating unique, synthesised, deepfake images (Cross, 2022).

1.3.3.2 Investment Scams

The fraudster, promising a high return, convinces their victim to transfer money to a non-existent fund or to pay for a non-legitimate investment in, for example, cryptocurrency or property. Often, the report to the police or the bank will be made by a concerned friend or family member. A

challenge for police officers dealing with instances of investment scams (and romance scams) is that the victim may be in denial regarding the possibility the investment opportunity is not real.

Though the method of deception may vary with each scam, the common theme with APP fraud is that the fraudster purports to be someone they are not and tricks their victim into completing a financial or informational transaction. In other types of cybercrime and online fraud, the offender will gain unauthorised access and complete the transaction themselves (though often with the assistance of the victim who has been deceived).

1.3.3.3 Tech Support Scams

Tech support scams involve fraudsters posing as technical support representatives from a reputable company, and advising victims of supposed issues with their computer or software. The scammer convinces the victim to grant 'remote access' to their device or provide payment for non-legitimate services. Once access is gained, the fraudster may steal data or transfer funds to their own account.

1.3.3.4 Account Takeover (ATO) Fraud

ATO amounts to identity theft and occurs when a fraudster accesses their victim's login credentials and gains access to, for example, their bank, social media or email account. This can be achieved by means including mail theft, phishing, malware (harmful software installed without knowledge (FTC, 2024)) or 'man-in-the-middle' attacks (where communications are intercepted). On gaining access, the fraudster can engage in fraudulent activities, including unauthorised purchases, transferring funds to their own account, and launching phishing attacks on the victim's contacts. Phishing is "when criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information" (NCSC, 2021).

1.3.3.5 *Internet of Things Device Exploitation*

The proliferation of Internet of Things (IoT) devices, such as smart home appliances and wearable technology, presents opportunities for cybercriminals to exploit vulnerabilities and carry out fraud. Scammers can obtain access to IoT devices to gather personal data, intercept communications, or manipulate physical environments (e.g., adjusting thermostat settings or locking doors) to extort money from victims.

1.3.3.6 *Deepfakes and Artificial Intelligence (AI)*

Deepfake technology, which uses artificial intelligence to create highly realistic non-legitimate videos or audio recordings, can be used to perpetrate scams by impersonating individuals or manipulating content to deceive victims. AI-powered chatbots have the potential to revolutionise customer service and support interactions but can also be used illegitimately to impersonate trusted individuals or organisations and manipulate victims into disclosing sensitive information or making financial transactions. These sophisticated chatbots could employ natural language processing and machine learning algorithms to mimic human conversation and evade detection.

1.3.4 *Factors associated with cybercrime*

The question of who is commonly affected by which type of cybercrime, how and how often, must account for the multitude of cybercrime types, severities, mediums, and contexts. Underreporting by different demographics or people with different characteristics, for example because of shame or embarrassment or a lack of knowledge around what constitutes different offences, may skew our understanding of cybercrime epidemiology (Reep-van den Bergh & Junger, 2018; Reyns & Englebrecht, 2010).

1.3.4.1 *Relationship to age*

The relationship between age across the life course and cybercrime victimisation is unclear, in part because many studies focus on young internet users and use university students or

adolescents as participants (e.g. Bossler & Holt, 2010; Hasan et al., 2015; Kaakinen et al., 2018; Longobardi et al., 2020). Those studies with samples spanning larger age ranges tend to conclude that younger people are more at risk than older people (e.g. van de Weijer & Leukfeldt, 2017), the primary reason being their greater exposure to malicious actors online as a result of their greater internet use and online interactions and greater propensity to engage in risky behaviours (Leukfeldt & Yar, 2016; Mikkola et al., 2024). The picture is more nuanced when investigating specific crime types, however. Oliveira et al. (2017), for example, found that older women were more susceptible to spear phishing (whereby fraudsters target malicious emails at a specific person, as opposed to hoping for a 'bite' from one of many recipients), and van de Weijer et al., (2019) found that age was positively correlated with reports of hacking incidents, though they attribute this to underreporting of hacking among younger demographics for whom it is a more common and less serious occurrence. The hypothesis of this thesis is that there may be important differences in how and in what contexts older people experience and respond to cybercrime, compared with younger people, as evidenced in Burton et al.'s (2022) realist review.

1.3.4.2 Relationship to gender

The relationship between cybercrime victimisation and gender varies by cybercrime type. Whitty (2018) found that romance scam victims are more likely to be women, whilst Kaakinen et al., (2021), who examined online dating victimisation experiences among adolescents of various nationalities, found that experiences of online harassment and aggression victimisation was more prevalent among males but that females were more likely to experience online offences of a sexual nature. Other research indicates that women are more susceptible to phishing than men (Halevi et al., 2015; Lin et al., 2019), but that men are more likely to be victims of online financial fraud (Garlicki & Mider, 2022).

1.3.4.3 *Relationship to ethnicity*

There is limited research on the association between ethnicity and cybercrime victimisation. In an analysis of an earlier wave of Crime Survey for England and Wales data than the wave I analysed in the first study of this thesis, Brunton-Smith (2017) investigated the role of ethnicity and other demographic characteristics on fear of cybercrime, finding that Black, Asian and minority ethnic respondents have significantly higher odds (OR 1.57) of worrying about online crime. Näsi et al. (2015) surveyed participants from four Western nations and found that second generation immigrants were significantly more likely to be victims of cybercrime than everyone else. Regarding fraud, which shares a significant intersection and many similarities with cybercrime, Raval's (2021) postulated that individuals of Black ethnicity from communities with high ethnic density may be more likely to experience financial difficulties, and therefore be more likely to engage with potentially fraudulent lenders or debt relief services. This was not true of Asian or Hispanic communities.

1.3.4.4 *Relationship to education*

The relationship between level of education and cybercrime victimisation is complex. In theory, those with a greater educational attainment might be more knowledgeable about cyber threats and how to avoid and manage them effectively (Yucedal, 2010), though higher educational levels may also be associated with increased use of digital devices and therefore exposure to malicious actors (van de Weijer et al., 2019). Survey analyses carried out internationally (Näsi et al.'s 2023), in Nigeria (Ndubueze et al.' 2013) and in Germany (Bergmann et al.'s 2018) revealed no clear or consistent association, though the latter did find that people with a high or middle education had a higher risk of experiencing 'misuse of personal data' – the examples given being phishing and identity theft – than people with a low educational level. Contrastingly, van de Weijer et al. (2019) found that educational level is significantly negatively correlated with reporting victimisation of identity theft, consumer fraud and hacking.

1.3.4.5 Relationship to health

It is well documented that cybercrime victimisation can cause poor mental and physical health (discussed in section 1.2.5), but fewer studies have explored the reverse, that poor mental and physical health are victimisation risk factors. In investigating the correlates of susceptibility to fraud and scams among community-dwelling older adults, both Yu et al. (2021) and Judges et al. (2017) found a strong association with lower susceptibility and better cognitive health, which Judges et al. suggest may be related to attention lapses and difficulties comprehending language increasing risk. There is a dearth of evidence on the link with physical health, although Burton et al. (2022) theorise that “if an older adult experiences declining health and mobility they may rely more on online banking, shopping, health care and social media services, sharing personal details more frequently, resulting in increased online visibility and risk of victimisation”. Yu et al. (2021) identified no correlation between physical health and scam susceptibility, though they note that their sample was probably disproportionately healthy. Several studies point to the reciprocal nature of the relationship between health and cybercrime victimisation. Regarding cyberbullying, Gámez-Guadix et al. (2013) suggest that depressed individuals may lack social skills and tend to isolate, consequently accessing less peer supports and are therefore more likely to be victimised. This, in turn, might cause loneliness and further depression.

1.3.4.6 Relationship to other socio-economic factors

Multiple studies have revealed that online victimisation is predicted by offline victimisation (e.g. Helweg-Larsen et al., 2012; Ioannou et al., 2018; Mitchell et al., 2011), commonly explained by the increasing integration of technology into day-to-day life and consequent flow and continuity of events between physical and digital realms (Awan & Zempi, 2016). Whereas several studies indicate that offline victimisation is predicted by a poor financial position (e.g. Tilley et al., 2011), Näsi et al. (2023) found that people in a better financial position are more likely to be victims of cybercrime, possibly because they are more active internet and device users. There is limited

research regarding employment as a risk factor of cybercrime victimisation, although Ngo & Paternoster's (2011) found that, among university students, full or part-time employment was associated with lesser odds of experiencing defamation and online harassment from a stranger, presumably the result of having less leisure time to socialise online.

1.3.5 Impact of cybercrime on businesses

Most estimates regarding cybercrime impact exist in relation to businesses rather than individuals. Estimates of the extent of cybercrime tend to focus on the cost of cybercrime rather than the incidence or prevalence of exposure, especially beyond the individual level as almost all businesses will be affected to some extent. Cybercrime incurs indirect costs in the form of lost revenue, legal fees, remediation expenses, regulatory fines and rising insurance premiums (Saeed et al., 2023; Shah et al., 2019). The UK Government Cyber security breaches survey 2024 found that 50% of businesses experienced a cybersecurity breach in 2023, with phishing by far the most common type of attack (Department for Science, Innovation & Technology, 2024a). The survey estimates UK businesses experienced approximately 7.78 million cybercrimes of all types in the previous 12 months, with the most disruptive breach experienced by each business costing £1,205 on average in short term costs only. A 2011 UK Cabinet Office report estimated the general cost of cybercrime in the UK to be £27 billion per annum (Cabinet Office, 2011). More recent figures from UK government sources are not available.

1.3.6 Impact of cybercrime on individuals

Prevalence estimates of cybercrime are primarily obtained from police statistics (or in the UK, from partner agencies including Action Fraud, UK Finance and the Serious Fraud Office), or through independent or statutory victimisation and breach surveys (Breen et al., 2022). In the UK, data from the 2021/22 Crime Survey for England and Wales (CSEW) indicates that fraud and cybercrime “affect more people, more often than any other crime and represent 44% of all estimated crime” (Home Office, 2023). The cost of cybercrime to citizens in the UK has been

estimated at £3.1bn per annum (Cabinet Office, 2011). In the USA, 53.35 million citizens were affected in the first half of 2022, whilst one in two internet users experienced an account breach in 2021. The most common cyber threat facing individuals in the US is phishing (Griffiths, 2024).

1.3.6.1 The psychological impact of cybercrime

As with traditional crime victimisation, cybercrime victimisation can be a traumatic experience capable of causing short-term or prolonged psychological harm. Merryweather (2021) found that “being a victim of fraud was associated with significantly higher levels of anxiety and lower levels of happiness”, whilst Tripathi et al. (2019) noted in a qualitative study that victimisation could cause anxiety, depression and shame. Pandian & Maraimalai (2024) examined the impact of online harassment, cyberbullying, misinformation and exposure to explicit content on women, finding that these crimes can cause distress, anxiety, shame, avoidance, and fear. Cybercrime victimisation has also been linked to Post-Traumatic Stress disorder (PTSD). Worsley et al.'s (2017) survey of cyberstalking victims, for example, described post-traumatic stress symptoms including vivid flashbacks, intrusive recollections, disabling anxiety, paranoia, mistrust and panic attacks attributed by participants to their harassment or abuse online.

1.3.6.2 Somatisation

Somatisation is “the tendency to experience psychological distress in the form of somatic [relating to the body as opposed to the mind] symptoms (...) which may be initiated and/or perpetuated by emotional responses such as anxiety and depression” (Busaidi, 2010:180). Multiple studies make reference to victims of cybercrime experiencing physical symptoms brought on by their psychological state. Button et al. (2014), for example, spoke to victims of fraud who revealed they had developed skin conditions because of the worry their victimisation had provoked, whilst Cross et al. (2016) interviewed victims of fraud who reported experiencing weight loss and nausea. This reflects findings around traditional crime victimisation; Norris &

Kaniasty (1994) found that victims of violent and property crime commonly suffered symptoms of somatization, alongside depression and fear.

1.3.7 Procedures for reporting cybercrime

Action Fraud is the UK's national reporting centre for cybercrime and fraud, operated by the City of London Police in partnership with the National Fraud Intelligence Bureau (NFIB). It is a central point of contact for individuals and businesses to report cyber incidents, online fraud, and other types of economic crime (Action Fraud, 2019). Reports are collated and analysed to identify trends, patterns, and emerging threats in cybercrime (Action Fraud, 2019b) and data is often shared with law enforcement agencies, government bodies and industry partners to facilitate intelligence-led policing, target cybercriminal networks, and disrupt criminal activities (Action Fraud, 2019a). Action Fraud also raises public awareness about cyber risks and fraud prevention through education campaigns and outreach initiatives, disseminating actionable advice and guidance (e.g. Action Fraud, 2024). Action Fraud supports victims of cybercrime, providing guidance on reporting the incident, accessing support services, and recovering from financial losses (Action Fraud, 2019c). Upon receiving a report, Action Fraud conducts an initial triage and assessment to determine the nature and severity of the incident, and whether it is suitable for referral to law enforcement agencies for further investigation, action, or intelligence gathering purposes (North Yorkshire Police, 2024). Action Fraud has been subject to significant criticism for several years, with the UK Parliament Justice Committee describing it as “unfit for purpose”: Sir Bob Neill, chair of the Justice Committee, stated in 2022 that:

Fraud currently accounts for 40% of crime and the figure is growing. People are losing their life savings and suffering lasting emotional and psychological harm. But the level of concern from law enforcement falls short of what is required.

The decision has already been made to replace Action Fraud, and the Government will need to make sure its successor can meet the demands placed on it, but the wider

criminal justice system must also renew its focus on this crime. Fraud prevention, investigation and prosecution too often has seemed like an afterthought, last in the queue for resources, monitoring and even court time.

We need the criminal justice system to have the resources and focus to be able to adapt to new technologies and emerging trends. The current sense of inertia cannot continue, we need meaningful action now (UK Parliament, 2022).

The replacement service, operated by Capita PLC and PWC UK on behalf of the City of London Police, was due to launch in the second quarter of 2024 (City of London Police, 2023a), but this has been delayed until 2025 (Martin, 2024).

In the UK, banks and financial institutions have protocols in place to address instances of financial fraud and reimburse victims. The UK's Payment Services Regulations established the liability framework for unauthorised transactions, outlining the circumstances under which banks are responsible for reimbursing victims of fraud (legislation.gov.uk, 2017). Until 07 October 2024, there had not been any requirements for banks to recompensate victims of fraud; this was done voluntarily under the Contingent Reimbursement Model code (LSB, 2024), of which multiple major banks and building societies were signatories (Refundee, 2024). Now, Banks are generally obligated to refund victims for unauthorised transactions, provided that the victim has not acted fraudulently or with gross negligence (Tennant, 2025). UK banks typically have procedures for investigating reported cases of financial fraud. Victims are encouraged to report fraudulent transactions to their bank as soon as possible to initiate the reimbursement process. Banks may conduct investigations to verify the authenticity of the fraud claim and determine the appropriate course of action. Upon confirmation of fraud, victims are typically reimbursed for the full amount of the unauthorised transaction, although the reimbursement process may vary depending on the circumstances (HM Treasury, 2024). If the bank or financial institution has concerns about the welfare or capacity of the customer, they may request a welfare check or

intervention from the police or relevant authorities. This is known as the Banking Protocol scheme (Action Fraud, 2020), and could include cases where the customer appears to be vulnerable, isolated, or incapable of making sound financial decisions due to illness or cognitive impairment (Age UK, 2018).

1.3.8 Cybercrime reporting decision making

Cybercrime may be particularly likely to be underreported (e.g. ISACA, (2019)) in comparison with traditional crime. A study by Wall (2008) suggested that victims may consider cybercrime less worthy of reporting than traditional crime because it is informational rather than physical. Though Graham et al. (2019) acknowledge that internet users are now much more familiar with, and willing to report, online offences, they propose that victims believe the likelihood of arrest is significantly greater for traditional crime than for cybercrime. Correia (2022) claims that victims may not see the benefit in reporting as they anticipate an ineffective response. Other proposed reasons behind cybercrime underreporting include victim embarrassment (Abdulai 2020; (Jaishankar, 2020)) and a lack of knowledge regarding what constitutes an offence, where and how to report it (Bidgoli and Grossklags 2016).

1.3.9 Cybercrime prevention and protection

1.3.9.1 Law enforcement and cybercrime

In UK law, cybercrime is not an offence in itself, but rather an umbrella term that encompasses both cyber-enabled crime and cyber-dependent crime:

Cyber-dependent crime (crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime); or cyber-enabled crime (crimes that may be committed without ICT devices, like financial fraud, but are changed significantly by use of ICT in terms of scale and reach) (CPS, 2024).

Cyber-enabled crime describes ‘traditional’ crimes, such as fraud and theft, that have been facilitated by Information Computer Technology (ICT). Such offences will be charged under the relevant ‘traditional’ legislation, such as the Fraud Act 2006 or the Theft Act 1968. Cyber-dependent crimes can only be committed using ICT. Examples include hacking and Denial of Service (DOS) attacks, and such offences are prosecuted under the Computer Misuse Act (CMA) 1990 or, in some instances, the Investigatory Powers Act (IPA) 2016.

There are a number of national and regional statutory organisations charged with addressing cybercrime in the UK, from a national to local level. The National Cyber Security Centre (NCSC), launched in 2016, is the technical authority for cyber threats and forms part of the UK Government Communications Headquarters (GCHQ). It is the chief coordinator of the UK’s response to cybercrime, with responsibilities including: monitoring incidents; providing early warnings; disseminating information, conducting cyber threat assessments; and providing general technical support to different authorities. It also leads the UK’s cybersecurity international co-operation (ICO, 2024b). The National Crime Agency (NCA) is the UK’s leading law enforcement agency responsible for tackling serious and organised crime, including cybercrime. The NCA’s Cyber Crime Unit (NCCU) is tasked with investigating cyber threats, disrupting cybercriminal networks, and supporting law enforcement efforts to combat cybercrime (NCA, 2020). Regional Organised Crime Units (ROCU), of which there are nine across England and Wales – each one being affiliated with three or more constituent police forces (ROCU, 2024) – exist to tackle cross-county organised crime. They provide a range of specialist capabilities to forces including covert operations, surveillance, intelligence and cyber (HMICFRS, 2021). ROCU cybercrime units work in partnership with the NCA and NCSC both proactively and reactively, on cyber investigations, defending against threats, deterring and disrupting hostilities, and on building cyber resilience (ROCU, 2024a).

On a local level, each police force is responsible for investigating reports of fraud and cybercrime directed from Action Fraud, and providing advice to businesses and members of the public (City of London Police, 2023b). The Metropolitan Police Service's Cyber Protect Team, for example, was set up "to help protect small to medium-size businesses and charities from the ever-growing threat of cybercrime. [They] provide advice, presentations and planning exercises with businesses and charities to raise awareness of cyber threats and help organisations protect themselves" (MPS, 2021).

The Banking Protocol is a national scheme launched by National Trading Standards, UK Finance and local police services. Staff within UK bank branches are trained to detect red flags that indicate a customer may be being targeted by fraudsters (not exclusively online), and alert police. Customers are then supported to recover from their victimisation and protect themselves against repeat victimisation.

The majority of victims being targeted are elderly and vulnerable people. The Banking Protocol also ensures that extra support is provided to customers identified through the scheme, to help prevent them from falling victim to similar scams in the future. This can include referrals to social services, expert fraud prevention advice and additional checks on future transactions (West Mercia Police, 2021).

In 2022, £55.5m of fraud was prevented thanks to the Banking Protocol scheme (UK Finance, 2023). The new rules, described above mean that it has been mandatory for banks to reimburse fraud victims since October 2024, allowing Payment Service Providers (PSPs) to apply an excess of up to £100, and if there is significant evidence of gross negligence then the victim will be rendered ineligible. However, neither the excess nor the negligence exception applies to vulnerable consumers. The Payment Systems Regulator (PSR) defines a vulnerable consumer as:

Someone who, due to their personal circumstances, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care. PSPs should evaluate

each customer's circumstances on a case-by-case basis to help determine the extent to which their characteristics of vulnerability, whether temporary or enduring, led them to be defrauded, and therefore whether they meet the definition of vulnerability (PSR, 2023).

1.3.9.2 Organisational cybersecurity

With half of UK business reporting cyber breaches in the last year (Department for Science, Innovation & Technology, 2024a), cybersecurity has become an elemental part of organisational operations. The UK Government's Cyber Code of Practice recommends a multipronged approach: Risk Management (i.e. security assessments and addressing risks); Cyber Strategy (i.e. developing capabilities to manage threats and reviewing resilience against changing contexts); People (i.e. fostering cyber security culture and providing employee training); Incident Planning and Response (i.e. plans to recover from critical cyber incidents); and finally Assurance and oversight (i.e. implementing a cyber resilience governance structure and clear monitoring process) (Department for Science, Innovation & Technology, 2024b). Legally, businesses must comply with UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, which mandate the use of 'appropriate' measures and adherence to data protection principle (NCSC, 2023). If non-compliance is detected, the Information Commissioner's Office (ICO) – the UK's independent authority responsible for enforcing data protection law – can issue penalties (ICO, 2024c). Public and private sector organisations must abide by this legislation. The ICO recently reprimanded the Council of the London borough of Hackney following a cyber-attack in 2020 in which hackers accessed over 400,000 files containing personal data of residents (ICO, 2024a).

1.3.9.3 Individual cybersecurity

In North America, one in two internet users had their accounts breached in 2021. Meanwhile, the UK had the highest number of cybercrime victims per million internet users of any country, at 4783 in 2022, up 40% from figures for 2020 (Griffiths, 2024). The National Cyber Security Centre

offers a cybersecurity ‘action plan’ to members of the public, which asks a series of questions regarding one’s cyber behaviours and proposes tailored cybersecurity measures accordingly, such as backing up data, changing passwords and turning on multi-factor authentication (MFA). MFA is “a security feature that requires you to verify your identity in multiple ways before accessing an account. (...) When logging in, you provide your username and password as usual, but then you add another step to prove it’s really you. This second step could be a fingerprint, a code sent to your phone, or even a notification from an app” (National Cybersecurity Alliance, 2025). Much of the research around cybersecurity measures for individuals relates to *usability*, and the fundamental dilemma around bolstering cybersecurity is how to balance increasingly technical means with usability (Grobler et al., 2021). Braz & Robert's (2006) review of MFA usability, for example, remarks on the overcomplexity of password requirements, combined with biometric enrolment processes and “cumbersome” data input requests which may reduce inclusivity.

1.3.10 Cybercrime offenders

Payne et al. (2019) investigated the differences between cybercriminals and ‘traditional’ criminals using the FBI’s most wanted list, finding that cyber offenders tended to be younger, white-collar professionals, predominantly male and of white ethnicity. This contrasts with traditional criminals, who may come from a broader range of backgrounds and age groups. Cyber criminals also possessed higher levels of education, particularly in fields related to technology and computer science. This study also found that cyber criminals are more likely to be driven by financial gain, whereas traditional criminals are driven by a range of factors, including social or psychological gratification. Consistent with Payne’s findings are those of Weulen Kranenbarg et al. (2018), who analysed mandatory resident ‘registration’ data in the Netherlands from 2000 to 2012 and found that employment and education were associated with the likelihood of committing a traditional, but not a cyber offence. Schiks et al. (2022) investigated the intellectual capabilities of cyber offenders in comparison with traditional offenders and people who have

never been convicted of an offence. The authors found that cyber offenders had intelligence test scores that were higher than traditional offenders, but lower than the general population. Lim et al. (2023) found that individuals with Autism Spectrum Disorder, a neurological and developmental disorder that affects how people interact with others, communicate, learn, and behave (NIMH, 2025), were more likely to engage in cybercrime than non-autistic individuals, but that this relationship was not mediated by advanced digital skills or deficits in theory of mind – despite theory suggesting that autistic people have greater capacities around advanced information technology (Baron-Cohen et al., 2003). In summary, cyber criminals are somewhat ordinary – with no particularly discernible traits - which serves to strengthen their anonymity and make difficult their detection.

1.4 Ageing

The UK has an ageing population; the number of people aged 65 years and over increased from 9.2 million in the 2011 census to over 11 million in the 2021 census (ONS, 2023a). This is explained by increasing life expectancy driven by advances in healthcare, declining birth rates (Foster, 2018), and the natural demographic transition of post-war ‘baby-boomers’ (Hodge, 2016). Globally, the world’s population of people aged 60 plus is set to more than double between 2020 and 2050, from 1 billion to 2.1 billion, and the number of people aged 80 plus is expected to triple over the same period (WHO, 2024) to around 426 million.

1.4.1 Sociological theories of ageing

A number of attempts have been made to divide the ageing process into distinct stages. The ‘third age’ and ‘fourth age’ are widely referenced gerontological constructs to consider the ageing experience. The third age refers to the period of life following retirement, typified by relative health, independence, and active engagement in various activities. This stage is often associated with opportunities for personal fulfilment, social participation, and continued productivity, allowing individuals the autonomy to pursue interests and hobbies that may have been set aside

during their working years. The fourth age follows the third age and represents a notable decline in an individual's physical health and cognitive function and a greater level of dependency on others. Loss of health can cause loss of mobility, and when combined with bereavements, can be associated with loneliness. A metanalysis of observational studies from high income countries between 2008 and 2020 revealed that a quarter of older adults aged 60 or more experience some loneliness (Chawla et al., 2021). Loneliness and social isolation have been linked to cognitive decline and a higher risk of dementia (National Institute on Aging, 2024).

Whilst the third and fourth age concepts allow for a more nuanced understanding and treatment of ageing, critics argue that a focus on successful ageing in the third age can inadvertently marginalise those in the fourth age, which has become a relative 'black hole' of "disability, diminishment and death" with few attempts to really understand it (Gilleard & Higgs, 2010:126). An alternative perspective is Erik Erikson's Stages of Psychosocial Development, which posits eight sequential stages of individual development, and a further ninth offered by Joan Erikson (Gross, 2020). The eighth and ninth stages focus on older age. The eighth is characterised by a tension between feelings of 'ego integrity' – a state of mind supported by an inner sense of productivity and meaningfulness – and feelings of despair, resulting from regret and shortness of time remaining. The ninth stage offers several new conflicts, such as mistrust in one's own physical abilities, questions over autonomy, and doubt in one's existential identity, status and role. Critics of Erikson's stages cite its bias towards values like independence, autonomy, and productivity, deeply ingrained in Western individualistic cultures. The theory may not translate well to more collectivistic cultures that value interdependence, social harmony, and shared responsibility (McLeod, 2024).

1.4.1.1 Ageism

'Ageism' was a concept first introduced by Butler (1969:243) in its simplest terms as "prejudice by one age group toward other age groups"; Butler later expanded this definition (Butler, 1980):

1) Prejudicial attitudes toward the aged, toward old age, and toward the aging process, including attitudes held by the elderly themselves; 2) Discriminatory practices against the elderly, particularly in employment, but in other social roles as well; and 3) institutional practices and policies which, often without malice, perpetuate stereotypic beliefs about the elderly, reduce their opportunities for a satisfactory life and undermine their personal dignity (Butler, 1980).

Ageism can also be self-perpetuating; older adults may internalise – and fulfil - widely held societal beliefs or expectations about how they should or shouldn't behave (Giles & Reid, 2005). Such behaviours are then observed by society as evidence of ageist stereotypes – an example of a 'self-fulfilling prophecy' (Madon et al., 2011). Ageism has been linked to adverse health outcomes including depression, stress, low self-esteem (Ng et al., 2022) as well as social exclusion and isolation (Kornadt et al., 2021).

1.4.1.2 Digital ageism

Though the benefits of internet use – despite the threat of cybercrime – are clear, 'digital ageism' can impede older adults' propensity to capitalise on the internet and digital technology. Digital ageism has been defined by Rosales et al. (2023) as "the implicit or explicit discrimination of older adults based on how age is represented and experienced in relation to digital technologies". It is an emerging concept that encapsulates the discrimination and bias against older adults within the digital landscape, particularly as technology becomes increasingly integral to everyday life. It can manifest in various ways, impacting older individuals' access to technology, their representation in digital media, and their overall engagement with digital platforms. Pervasive, ageist, victim blaming societal attitudes can discourage reporting of cybercrime due to shame and fear of losing independence, and digital ageism may operate through unsuitable digital technology design and provision within the Fraud Justice Network (FJN)

– Button et al.'s (2013) collective term for the multiple agencies available for reporting cybercrime.

Rosales et al. (2023) propose that digital ageism operates on corporate and interpersonal levels. Corporate biases describe the under-representation of older adults within institutions that make digital technology, and the design, development, testing and advertising of their products. Interpersonal biases refer to societal stereotypes regarding age in relation to technology. For example, the idea that older adults are digital 'immigrants' and 'late adopters' rather than natives and 'early adopters' fails to acknowledge that no digital skills are innate, but acquired through access, interest and practice. The portrayal of older adults as inherently digitally challenged predicates against empowerment, and provision of products appropriate to their needs, so these biases are self-perpetuating (Rosales et al. 2023). There is presently no published research exploring digital ageism within fraud and cybercrime reporting mechanisms.

Berridge et al. (2022) highlight how neglect of older adults' needs in technology design leads to a lack of user-friendly interfaces, which can exacerbate the digital divide. Rosales and Fernández-Ardèvol argue that ageism is systemic; embedded in the corporate cultures of technology companies, resulting in discriminatory practices that deprioritise older users (Rosales & Fernández-Ardèvol, 2020). Ivan et al. (2020) discuss "visual ageism", which refers to the prejudiced representation of older individuals in visual media, often depicting them in negative or stereotypical ways. Such representations can influence public perceptions and reinforce ageist attitudes, further marginalising older adults in digital spaces. The implications of these portrayals are profound, as they contribute to a societal narrative that undermines the value and contributions of older individuals.

Chu (2024) emphasises that biases in AI systems can lead to the exclusion of older adults from critical services, particularly in healthcare, where age-related biases in algorithms can affect the quality of care they receive. This concern is also voiced by Stypińska (2022), who identifies

multiple forms of ageism in AI, including technical biases and the invisibility of older adults in digital discourses. Research indicates that exposure to ageism can lead to decreased self-efficacy regarding technology use, further entrenching the digital divide (Choi et al., 2020).

1.4.2 Healthy and successful ageing

The World Health Organisation (WHO) defines healthy ageing as the process of developing and maintaining the functional ability that enables wellbeing in older age. Functional ability is having the ability to: meet basic needs; be mobile; learn, grow and make decisions; build and maintain relationships; and contribute to society (Rudnicka et al., 2020). Successful ageing has significant overlap with healthy ageing in that physical and mental health are elemental. However, successful ageing is a much broader term that incorporates considerations such as purpose and engagement as indicators of prosperity. Commonly proposed features of successful ageing include absence of disease, productive social engagement, engagement in physical activity, and feelings of purposefulness and inner happiness (Estebarsari et al., 2020). Livingston et al. (2008) argue that successful ageing is also maintaining a positive outlook despite poor health, and that older people can still live successfully with physical or cognitive impairment. They found that in people with dementia, wellbeing was predicted by social relationships and absence of anxiety and depression, rather than by dementia severity or general health. Bone et al.'s (2022) examination of the association between leisure activities and depression found that attending sport, social or other clubs was consistently associated with reduced odds of depression. Lee et al.'s (2019) investigation into the effect of retirement and leisure activity engagement on cognition revealed a negative association between retirement and cognition, attenuated by engagement in mental activities such as reading newspapers and books, playing cards or games, solving puzzles and singing or playing music.

Chronological age, the principal way in which humans define age, refers to the duration of time lived. Biological age is an amalgamation of different biological and physiological development

factors, including chronological age, genetics, lifestyle, nutrition, diseases and other conditions, which can provide a more accurate estimate of a person's stage and health (Frothingham, 2019). Biological age can be increased through physical activity and dietary changes (Fitzgerald et al., 2023; Leitão et al., 2022; Melk et al., 2014; Xu et al., 2024; Zhang et al., 2023). Brain age is an index for quantifying a person's brain health in comparison with a normal brain ageing trajectory (Vidal-Pineiro et al., 2021).

1.4.3 Wellbeing and illness in older age

1.4.3.1 *Frailty*

Frailty is a “clinically recognizable state of increased vulnerability resulting from aging-associated decline in reserve and function across multiple physiologic systems such that the ability to cope with every day or acute stressors is comprised” (Xue, 2011). Frailty may arise from conditions affecting physical, mental and/or cognitive health. In practice, for someone that is frail, a seemingly minor occurrence or issue, such as a fall, can have a severe long term effect on that person's health and wellbeing (Age UK, 2020). Symptoms of frailty include a diminished ability to care for self, sensory deterioration, fatigue, loss of strength, loss of mobility, and cognitive deterioration (Pel-Littel et al., 2009). Much of the recent research around frailty concerns life-course epidemiology (Hoogendijk et al., 2019); how adverse outcomes can be predicted through the identification of young-age risk factors such as obesity, malnutrition and even loneliness (e.g. Feng et al., 2017). There is little evidence around whether physical frailties are associated with cybercrime victimisation risk, though Burton et al. (2022) theorise that poor mobility might increase older adults' reliance on online services such as online banking, shopping and healthcare, resulting in increased exposure to cybercrime and therefore a heightened risk of victimisation.

1.4.3.2 *MCI and dementia*

Cognitive decline is common in older age, though it is not part of normal ageing. Mild cognitive impairment (MCI) is “the transitional state between the cognitive changes of normal aging and very early dementia” (Petersen & Negash, 2008). It is characterised by memory or thinking difficulties, though people with MCI can usually take care of themselves and carry out normal day to day activities (Alzheimers.gov, 2024). For some people, MCI symptoms might improve as they are often caused by a health condition, such as hearing loss or having low blood pressure, that can be treated (Alzheimer’s Society, 2023).

Dementia is “a term for several diseases that affect memory, thinking, and the ability to perform daily activities” (WHO, 2023a). There are approximately 982,000 people living with dementia in the UK – 57% of whom are women – and this figure is expected to rise to over 1.4m by 2040 (Carnall Farrar, 2024). Though the incidence of dementia increases in older age groups (Prince et al., 2014), approximately 7% of those with a recorded diagnosis of dementia in the UK are diagnosed before the age of 65 (NHS, 2024).

Mental disorders (most commonly depression and anxiety) account for 10.6% of disability adjusted life years among older adults. Antidepressant use by older people with depression is increasing (Arthur et al., 2019) but the condition remains under-recognised and under-treated (Cooper et al., 2010) and is more commonly resistant to treatment in this age group (Knöchel et al., 2015). Globally, around a quarter of deaths from suicide (27.2%) are among people aged 60 or over (WHO, 2023b). Depression may increase the risk of developing dementia (John et al., 2022).

1.4.3.3 *Metacognition*

Dementia usually affects decision making – the process of selecting an appropriate action from several possible actions – as well as one’s capacity – the ability to make a specific decision such as a financial decision, or to perform a specific task such as driving (Darby & Dickerson, 2017). A

self-awareness of deficits in decision making and capacity is called Metacognition, “an important practical skill that allows patients to adapt their behaviour so that events where impaired decision making are likely, occur less often” (ibid:272). Patients with most types of dementia have been shown to have impaired metacognition (Wilson et al., 2016). Cognitive impairment and loss of metacognition can lead to poor decision making. A study by Boyle et al. (2012) found that even subtle cognitive decline detrimentally effects decision making and judgement in relation to financial scams. Hsu & Willis (2013) found that among older couples, the individual responsible for their financial dealings will continue to manage their financial holdings long after they acknowledge having difficulties doing so, indicating a loss of metacognition.

1.4.4 Technology, internet use and aging

In recent years, internet use has rapidly increased among older adults (ONS, 2020). This can be linked to increased availability of digital technology (Kyaw et al., 2024), the closure of high street shops and services (Blomquist & Hägglund, 2021), the digitalisation of services such as healthcare (Sun et al., 2020), and the perceived social benefits of using the internet (e.g. participating in group conversations with family or friends) (Zhang & Li, 2022), all of which were accelerated by the COVID-19 pandemic in 2020 (Ferreira et al., 2022).

1.4.4.1 *Bridging the digital divide*

There remains a discrepancy between attitudes towards, and use of, the internet and digital technology between younger and older generations. Data from the 2019/2020 wave of a national internet use survey shows that 99% of adults aged between 16 and 44 in the UK were recent internet users, though the proportion for over 75s was just 54% (ONS, 2021). Lee et al.'s (2019) 20 year longitudinal survey of nearly 4000 adults revealed that comfort and efficacy using computers was lower in older age groups. Seeking to bridge the digital divide, Choudrie et al. (2020) investigated reasons for mobile phone adoption among older adults to inform business

policy and decision making. Their survey data revealed that the ability to capture or record moments to share with friends or family was a significant driver of mobile phone adoption, but that the absence of an individual to assist them was a likely deterrent, as was small screen size. Initiatives to boost technology adoption include ICT demonstration groups for older adults to learn, test and give feedback on digital products (Wu et al., 2015).

1.4.4.2 Technology and wellbeing

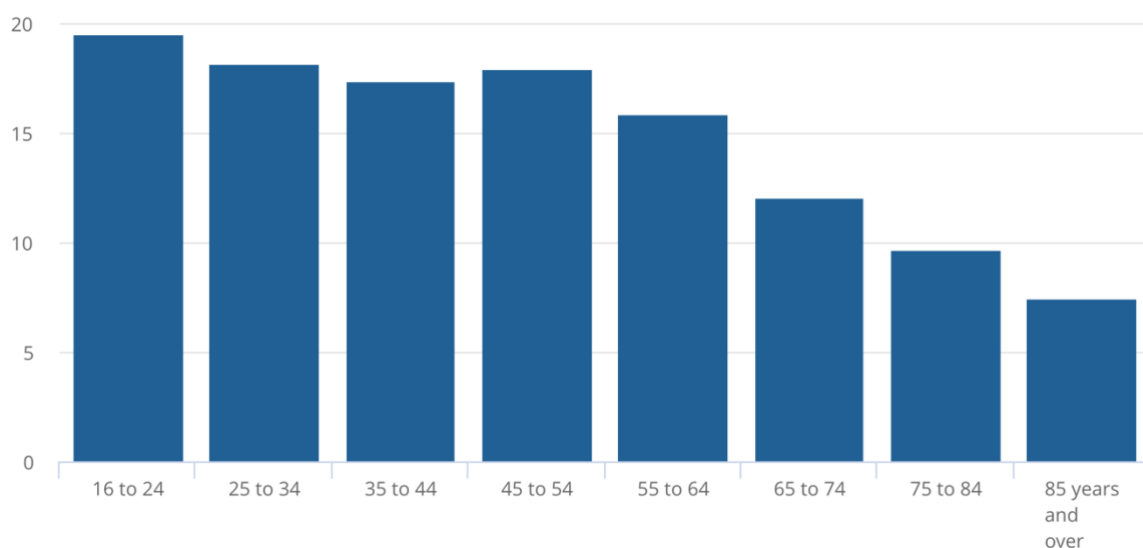
Technology allows the building and maintaining of social connections in older age (Cooper et al., 2021). Delello & McWhorter's (2017) found that iPads enabled older adults to maintain closer family ties and led to a greater societal integration, whilst Betlej's (2023) interviews with older adults about their experiences of ageing revealed that their primary motivation for using new technologies was sustaining social relations and networks. Participants also acknowledged a need to keep up to date with technology to maintain their independence, despite the challenge of constantly adapting to new devices and software updates.

The world wide web is an important source of healthcare information. Nam et al. (2019) examined the link between internet use among couples in later life and preventative health behaviours, finding that internet use was indeed associated with a higher likelihood of behaviours such as receiving flu shots, prostate exams and cholesterol tests. Technology allows remote communication between older adults and healthcare professionals and the monitoring of health indicators, empowering individuals to live as independently as possible in their own homes (Draper & Sorell, 2013). These remote care systems are often referred to as 'telecare', examples of which include two-way video displays, motion and temperature sensors (Taber-Doughty et al., 2010).

1.5 Crime and cybercrime against older adults

Crime victimisation is negatively correlated with age. Data from the 2022/2023 wave of Crime Survey for England and Wales data shows that the 19.5% of people aged 16 to 23 were once or more, victims of any crime, whilst the figure for individuals aged between 75 and 84 was 9.7%. Figure 1.2 shows the prevalence of victimisation in the Crime Survey for England and Wales by age group for the year ending March 2023 (ONS, 2024).

Figure 1.2. Crime victimisation by age group for the year ending March 2023 (ONS, 2024)



This trend tends to be attributed to the routine activities of younger individuals, who often engage in riskier behaviours and social environments that increase their exposure to potential offenders (DeCamp & Zaykowski, 2015). It also contradicts stereotypes around older adults being especially vulnerable to crime (Dias & Fraga, 2024).

It is unclear whether older adults or younger adults and children are more vulnerable to cybercrime specifically. Research on the subject suggests that young age is associated with cybercrime victimisation (Näsi et al., 2023; Van de Weijer & Leukfeldt, 2017), but this can plausibly be attributed to underreporting among older adults combined with greater activity online among younger demographics, which increases exposure to malicious actors (Koning et al., 2023). Older internet users are not a homogenous group, however.

It is possible that the majority of older adults are very cautious online so the risk of victimisation is low, but also there might be a minority of older adults with different characteristics who are particularly susceptible. For example, Crime Survey for England and Wales data shows that disabled people are more likely to be a victim of crime than non-disabled people (ONS, 2024), and census data shows that disability prevalence increases with age (ONS, 2023b). Furthermore, van Deursen & Helsper (2015) examination of internet use and non-use by older individuals found significant variations based on life stage, social environment, psychological characteristics, gender, education, and household composition (ONS, 2023b).

1.5.1 Victimisation risk factors among older adults

Multiple reasons have been proposed for why older adults are susceptible to cybercrime, or why they may be targeted by cybercriminals. By combining evidence from the body of relevant academic research with findings from consultations with expert stakeholders, Burton et al. (2022) developed a 'programme theory' to explain how and why older adults may be at risk of financial cybercrime through seven risk factors:

- Social Isolation

Social isolation is conducive to cybercrime victimisation and older adults may lack a protective social network. If an older adult is bereaved for example, lives far from friends and family, or has mobility issues, then it may limit their opportunities to seek help and advice. It might also cause loneliness, leading them to seek out connections online with new people, who may or may not be legitimate.

- Health vulnerabilities

When older adults are experiencing declining physical health, they may begin to depend more on online services such as shopping, social media and banking, resulting in greater online visibility.

If an older adult is experiencing cognitive decline then they might be less capable of assessing potentially fraudulent approaches and making appropriate choices under pressure.

- Memory loss

Memory loss could cause an older adult to forget key details about their victimisation (or about their victimisation entirely) resulting in insufficient information from which to launch an investigation, or in no report being made at all. Without police, bank or other support, repeat victimisation could occur. Related to this, Han et al. (2016) asked over 700 older adults without dementia to self-report on scam victimisation and undertake cognition assessments, finding that the presence and severity of cognitive impairment was associated with greater susceptibility to scams.

- Wealth

Older adults may have acquired significant and varied assets over time, making them a particularly attractive target for cybercriminals seeking considerable rewards for their effort. It could also mean that older adults may detect less rapidly if one of their many assets is compromised. UK Government data shows that from 2016 to 2020, the estimated average total wealth by age group was £66,000 for 25 to 34 year olds, £196,000 for 35 to 44 year olds, £364,000 for 45 to 54 year olds and £575,000 for 55 to 64 year olds (Social Mobility Commission, 2023). These figures encompass property, pension, physical health and financial wealth.

- Limited cybersecurity skills or awareness

If an older adult possesses limited tech savviness, they might not be fully aware of the risks on the internet, and they may be less inclined to stay up to date with the latest security advice. This naturally makes them more susceptible to the array of threats online. There may also be confusion around cybercrime reporting options; specifically who to report to in what circumstances.

- Societal attitudes

Ageist societal attitudes surrounding the supposed greed or gullibility of older adult victims of financial cybercrime may cause them to feel shame and embarrassment, or to fear that they will not be taken seriously. They are therefore less likely to disclose their victimisation to anyone, including the police, and are consequently unable to receive the support they need and more likely to fall victim to cybercrime repeatedly.

- Scam content developed by a motivated offender

Older adults may be more likely to engage with fraudulent approaches online if the scammer promises rewards, makes threats, or requests help. This is because these techniques illicit an emotional response. Additionally, if the scammer purports to be from a legitimate organisation such as a governmental department or a reputable business, the older adult may be more likely to succumb to their fraudulent requests because they have a greater trust in authority.

1.5.2 The impact of cybercrime on older adults

There is currently no research that quantifies the financial impact of cybercrime on older adults specifically, or in comparison with younger adults or children, though Tripathi et al. (2019) found that “money lost [by older victims of cybercrime in India] was part of their live savings and had been put aside for emergencies like medical treatments”. Indeed, such financial loss can be particularly impactful for older adults given they are unable to return to work in the same way that younger demographics could (Rabiner et al., 2006).

The psychological impact of cybercrime on older adults is well documented, however, and can be profound. Kemp & Erades Pérez's (2023) statistical analysis of a large sample of fraud victims showed that older adults were more likely than younger age groups to experience anger, embarrassment and negative effects on physical health brought on by stress. Meanwhile, Karagiannopoulos et al.'s (2021) interviews and focus groups with people over the age of 60 in

the UK, found that the trauma associated with cybercrime victimisation triggered a fear of internet use and use of online activities such as shopping and banking – which could otherwise drastically improve the quality of life for those with mobility issues or those who have retired in rural areas.

1.6 Summary

In my first chapter, I present a literature review, exploring existing literature surrounding cybercrime against older adults, and updating the literature published since Burton et al.'s (2022) realist review on this topic, which provided a theoretical foundation for this thesis, and led to my decision not to undertake a further, formal systematic review of the literature in this area. Instead, I introduced some of the key theories relating to crime and victimisation and their relevance to cybercrime and therefore this thesis. I have then discussed cybercrime, covering aspects including methods of categorisation, the impacts of cybercrime victimisation, and how organisations and individuals can protect themselves against cybercrime. Next, I have considered ageing and some of the sociological theories around ageing, including ageism and digital ageism. I have then looked at the meaning of healthy and successful ageing, before discussing some of the physical and psychological challenges of ageing. Finally, I have examined technology use in old age and the intersection between cybercrime and ageing.

Cybercrime is increasing (Fleck, 2024), as is internet use among older adults (Kung & Steptoe, 2023), and the impact of cybercrime can be particularly devastating for this demographic due to social, economic and health-related conditions associated with ageing (Satchell et al., 2023). Negative health outcomes range from shame and depression to hospitalisation and even mortality (DeLiema et al., 2017), and considering that certain vulnerabilities are more common in old age such as cognitive impairment, physical disability and lack of social support, there is a societal duty from researchers and practitioners to pay special attention to protecting this age group, collaboratively, from malicious actors online. Cybercrime is a relatively new challenge,

and digital ageism as a concept is just emerging, so the body of knowledge around multi-agency interventions to protect older adults and increase rates of reporting is extremely limited.

In Chapter 2, I will outline the structure of the thesis and main aims I wish to address through each of my three studies.

Chapter 2: Structure and aims of the thesis

2.1 Structure of thesis

This mixed-methods PhD comprises three studies, each of which informs the next, culminating in a series of recommendations on how to increase cybercrime reporting rates among older adults and a specific intervention proposal entitled ‘Online Porcupine’.

2.1.1 Study 1: Cybercrime victimisation among older adults: a probability sample survey in England and Wales

Study 1 is a quantitative analysis of the Crime Survey for England and Wales. In line with my thesis title, ‘Developing an Intervention to Protect Older Adults from Cybercrime’, I conceived this particular study to inform the development of tailored and targeted preventative measures for the conditions and contexts experienced by older populations which increase the likelihood of cybercrime victimisation, repeat victimisation and their consequences.

Aim: To explore how victimisation, repeat victimisation and financial impact are associated with age and other sociodemographic characteristics, and whether these relationships are influenced by economic and health-related factors and behaviours.

2.1.2 Study 2: Exploring the factors preventing older adults from reporting cybercrime and seeking help: a qualitative, semi-structured interview study

Study 2 is a qualitative, semi-structured interview study, designed to explore the barriers to reporting cybercrime among older adults. In view of the significant harms associated with

victimisation, including the impact of digital ageism, this study asks what prevents older adults from reporting their victimisation and receiving help and support, guided by Burton et al.'s (2022) programme theory and Rosales et al.'s (2023) interpersonal and corporate conceptual model of digital ageism.

Aim: To identify the barriers that older adults face when deciding whether to report cybercrime and to explore how they might be mitigated.

2.1.3 Study 3: Stakeholder workshops to generate intervention proposals for increased cybercrime reporting among older adults

To achieve this aim, I held four workshops with older adults and other potential intervention beneficiaries and implementers including police, health and social care professionals, and charity workers. During these workshops, we discussed the findings from my previous studies, as well as from the broader literature to conceive intervention ideas that would increase cybercrime reporting among older adults.

Aim: To consult with stakeholders on intervention proposals aimed at tackling barriers to cybercrime reporting to increase rates of reporting.

In the next chapter (Chapter 3), I present my first study; Cybercrime victimisation among older adults: a probability sample survey in England and Wales.

Chapter 3: Cybercrime victimisation among older adults: a probability sample survey in England and Wales

3.1 Introduction

Global digitalisation has increased the risk of cybercrime, and though the growing number of older people with online access has many positive benefits for society and individuals, it has increased exposure of this demographic group to cybercriminals (Cross, 2021). Risk factors that constellate in older age groups may be associated with greater susceptibility to cybercrime (Burton et al., 2022; Lin et al., 2019) as well as significant consequences for those who experience it. Crime victimisation in general can cause serious psychological harm to older adults in the form of anxiety, depression and even post-traumatic stress disorder (PTSD). Such harm may be exacerbated by factors such as pre-existing health conditions and social isolation (Satchell et al., 2023).

This study was conceived to inform the development of tailored and targeted preventative measures for the conditions and contexts experienced by older populations which increase the likelihood of cybercrime victimisation, repeat victimisation and their consequences. It is a quantitative analysis of data from the Crime Survey for England and Wales (CSEW). CSEW-based research on cybercrime is limited. Furnell and Dowling (2019) compared CSEW data with police statistics to offer “a portrait of the landscape”, considering the challenges involved with classifying and measuring cybercrime, and its associated costs and harms. Akdemir and Lawless (2020) used CSEW data and victim interviews to test the applicability of the Lifestyle Routine Activities Theory, an adapted form of the Routine Activities Approach which conceives risk of victimisation in terms of probability according to one’s overall lifestyle (Pratt & Turanovic, 2016). Similarly, Mikkola et al. (2024) conducted their own international survey of participants aged between 15 and 25 in order to investigate whether Routine Activities Approach can be used to explain risk of different kinds of cybercrime victimisation. None of these studies explored how

frailties and comorbidities associated with old age, including cognitive, mental and physical illness or social isolation, may influence victimisation. Poppleton, Lymperopoulou, and Molina (2021) conducted the only CSEW study to specifically address such vulnerabilities, yet their looks at fraud rather than cybercrime. Drawing on data from 2017 to 2019, they used victim and incident related risk factors and level of harm caused to divide England and Wales' general fraud victim population into nine demographic clusters, with older adults considered at particular risk.

There was, to my knowledge, no previous study investigating the relationship between age and cybercrime risk and impacts in a national sample. My aim was to explore how victimisation, repeat victimisation and financial impact are associated with age and other sociodemographic characteristics, and whether these relationships are influenced by economic and health-related factors and behaviours. I hypothesised that old age would predict cybercrime victimisation and repeat victimisation, and that older adults would be more likely to experience financial loss as a consequence of their victimisation, due to the risk factors associated with old age set out by Burton et al. (2022).

I have written a research article about this study, which was published in the scientific mega journal PLOS ONE on 18 December 2024. The article can be found at the following link:

<https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0314380>.

3.2 Materials and methods

3.2.1 Participants and procedures

The CSEW uses a multistage stratified sample and is administered via face-to-face interviews with more than 35,000 adults across England and Wales. It seeks to be representative of adults aged 16+ living in private households. Participants are randomly selected from the Royal Mail Postcode Address File. Participants are asked whether they have been a victim of crime(s) in the past 12 months, and other personal information on topics such as housing, work and health

(ONS, 2023). I analysed the 2019/2020 wave of data, collected in interviews held between April 2019 and March 2020. I did not seek Institutional ethics approval as Crime Survey data is publicly available from the UK Data Service, no participant is identifiable from Crime Survey data, and the authors had no contact with any participant at any stage.

3.2.2 Measures

3.2.2.1 Outcome measures

I defined Cybercrime using the ONS classification of cyber-related fraud and computer misuse, which mimics Home Office Counting Rules (Home Office, 2022) for recorded crime. Interviewers ascertained whether an offence was ‘cyber-related’ by asking the participant “thinking about the incident as a whole, was the internet, any type of online activity or internet-enabled device related to any aspect of the offence?” (ONS, 2019). Computer misuse offences include unauthorised access with intent to commit or facilitate commission of further offences (e.g. hacking into someone’s social media account in order to obtain personal data). Examples of cyber-related fraud include romance and investment scams. Given CSEW data is collected face-to-face, any participant uncertainties should have been resolved by the CSEW interviewer. The dichotomous primary outcome was whether participants reported being a victim of cyber-related fraud and computer misuse at all in the last 12 months. Dichotomous secondary outcomes were: (a) whether the participant was a repeat victim of fraud and computer misuse. To determine this, participants were asked whether they were victimised by incidents of fraud and/or computer misuse – not necessarily the same modus operandi – more than once during the 12 months prior to interview. The reference category here was individuals who had not been victim of fraud or computer misuse at all in the past 12 months; and (b) whether a participant who had experienced any victimisation in the past year experienced financial loss as a result of that victimisation.

3.2.2.2 Exposure variables

I included sociodemographic variables; and variables that reflect four of Burton et al.'s (Burton et al., 2022) seven risk factors: health vulnerabilities, memory loss, social isolation, and wealth. I was unable to include three risk factors – societal attitudes, scam content and cybersecurity skills or awareness – as the extent to which they are covered by CSEW variables is limited.

Sociodemographic/economic variables: I included age categorised in five bands: (16-24; 25-44; 45-64; 65-74; 75 and over); gender; and self-reported ONS harmonised ethnicity, reported in five categories (Table 1). I measured area deprivation using Indices of Multiple Deprivation (IMD). This combines information from seven domains (income deprivation; employment deprivation; education, skills and training deprivation; health deprivation and disability; crime; barriers to housing and services; and living environment deprivation). The resulting scores are translated into 'Lower-Layer Super Output Area' (LSOA: small geographical areas of approximately 1500 residents) deciles within the survey, which I converted into quintiles. I included tenure type, number of household members, hours spent away from home per weekday, and participant's most recent occupation.

Health variables: All health variables were self-reported. The first, 'status of health in general', was answerable with: 'Very good'; 'Good'; 'Fair'; 'Poor'; and 'Very poor'. Participants were asked to self-report the "presence of physical or mental health conditions or illnesses affecting the following areas": vision and hearing (here, grouped as 'sensory conditions'); mobility, dexterity, stamina or breathing or fatigue (grouped as 'physical conditions'); learning or understanding or concentrating, and memory ('cognitive conditions'); and lastly, mental health and 'socially or behaviourally' ('mental conditions').

3.2.3 Analysis

I performed all analyses using Stata 17. Where participants answered 'don't know' or 'not applicable' or refused to answer a question, the data was treated as missing. I excluded

participants who stated that they had not accessed the internet in the last year. I weighted data using the calibration weighting variable developed for the original CSEW survey design, designed to make adjustments for known differences in response rates between different age and gender sub-groups (ONS, 2020b), and report actual numbers and weighted percentages throughout.

I used standard summary descriptive statistics to characterise the sample (Table 1). In line with our aim to test how risk of cybercrime victimisation and repeat victimisation might be associated with age and health and social variables, I first investigated univariate associations of the exposure variables with primary and secondary outcomes (Table 1). Then, in two multivariate logistic regression analyses, I conducted forward stepwise logistic regressions with victimisation and repeat victimisation as the dependent variables, in which I entered variables in the following order: (1) sociodemographic and socioeconomic measures, (2) health measures.

To explore the association between age group and financial loss associated with cybercrime victimisation, I conducted a logistic regression with experience of financial loss as the dependent variable and age group as the independent variable (Table 2). For this analysis, I restricted our sample to people who had reported any cybercrime victimisation in the past 12 months; and investigated the proportion of respondents who had, and who had not reported related financial loss. Those not answering this question were excluded.

I was able to conclude from the results of this study that older adults may also be less able than younger adults to avoid repeat victimisation and financial loss, and may also be under-disclosing less serious victimisation (that does not involve repeat offences or financial loss) relative to younger adults in the CSEW, possibly mirroring a lower propensity to report cybercrime to the police, bank, or other authority. I remarked that future developments in platform and process design, as well as multi-agency collaboration and information sharing, should focus on empowering older adults to detect fraudulent activity before loss is incurred, and removing barriers to reporting.

3.3 Results

3.3.1 Sample description

Of the 36,913 participants in the survey, I excluded 738 who did not complete the primary outcome; and 1106 who reported that they had not used a computer in the past year (603 (54.52%) aged 75+, 292 (26.40%) aged 65-75, and 211 (34.99%) aged 16-64). The total analytic sample was therefore 35,069. Table 1 shows sample sociodemographic characteristics. Victimisation was reported by 2564 (7.31%) participants and repeat victimisation by 455 (1.30%) participants. 659 (25.70%) participants reporting victimisation answered the question regarding whether they had experienced financial loss as a result of their cybercrime victimisation, of whom 268 (40.51%) answered that they had experienced financial loss.

3.3.2 Findings

3.3.2.1 Associations with age

In fully adjusted multivariate models (Table 1 - which describes multivariate associations of variables with cybercrime victimisation and repeat victimisation) likelihood of cybercrime victimisation was highest among people aged 16-24 and lowest in people aged 75+. By contrast, repeat victimisation was experienced most frequently by people aged 75+, though this difference relative to the youngest age group (16-24) was not statistically significant. Meanwhile, adults aged 75+ were significantly more likely than participants aged 16-24 to experience financial loss as a result of their victimisation (Table 2).

3.3.2.2 Associations with other sociodemographic/economic exposures

In multivariate models that accounted for other exposures (Table 1), cybercrime victimisation (once or more times in the past 12 months) was associated with: being male or from a Black/African/Caribbean/Black British or mixed/multiple ethnic group; spending more time away from home on weekdays; having poor or fair mental health (as opposed to very good); and having

physical or mental health conditions. Individuals living in the most deprived areas were less likely to be victimised, as were those in all occupations but managerial and professional occupations, and individuals who reported having sensory health conditions.

Repeat victimisation (more than once in the past 12 months) was associated with: being male; being from a mixed/multiple or other ethnic group; and living in social rented rather than owned accommodation. Protective factors included being of Asian/Asian British ethnicity, holding an intermediate level occupation, being a full-time student, and having sensory health conditions.

Table 3.1. Sociodemographic characteristics of the sample and multivariate associations with cybercrime victimisation and repeat victimisation.

	Independent Variables	Total	Victimisation		Repeat Victimisation	
		N	n (%)	Odds Ratio (p)	n (% victimised) (% of total)	Odds Ratio (p)
AGE	Total	35069	2564 (7.31)	n/a	455 (17.75) (1.30)	n/a
	16-24	2343	214 (9.13)	ref	42 (19.63) (1.79)	ref
	25-44	11313	994 (8.79)	0.76 (0.009)	148 (14.89) (1.31)	0.64 (0.064)
	45-64	11922	970 (8.14)	0.65 (<0.001)	190 (19.59) (1.59)	0.90 (0.668)
	65-74	5249	273 (5.20)	0.40 (<0.001)	49 (17.95) (0.93)	1.13 (0.718)
	75+	4242	113 (2.66)	0.24 (<0.001)	26 (23.01) (0.61)	2.03 (0.074)
SEX	Female	18916	1314 (6.95)	ref	176 (13.39) (0.93)	ref
	Male	16153	1250 (7.74)	1.12 (0.020)	279 (22.32) (1.73)	1.78 (<0.001)
ETHNICITY	White	31092	2227 (7.16)	ref	394 (17.69) (1.27)	ref
	Mixed/Multiple	464	62 (13.36)	2.13 (<0.001)	21 (33.87) (4.53)	2.80 (0.011)
	Asian/Asian British	2181	152 (6.97)	0.96 (0.661)	13 (8.55) (0.60)	0.48 (0.034)
	Black/African/Caribbean/ Black British	1019	102 (10.01)	2.10 (<0.001)	19 (18.63) (1.86)	0.98 (0.945)
	Other	313	21 (6.71)	1.22 (0.450)	8 (38.10) (2.56)	7.37 (<0.001)
INDEX OF MULTIPLE DEPRIVATION	20% least deprived	7060	568 (8.05)	ref	104 (18.31) (1.47)	ref
	20%-40% least deprived	7322	576 (7.87)	1.03 (0.728)	89 (15.45) (1.22)	0.82 (0.318)
	40%-60%	7280	563 (7.73)	0.93 (0.296)	101 (17.94) (1.39)	1.02 (0.898)
	20%-40% most deprived	6978	476 (6.82)	0.79 (0.003)	101 (21.22) (1.45)	1.21 (0.301)
	20% most deprived	6429	381 (5.93)	0.73 (<0.001)	60 (15.75) (0.93)	0.97 (0.887)
HOUSEHOLD SIZE	Three or more members	12725	1049 (8.24)	ref	167 (15.92) (1.31)	ref
	Two members	12826	900 (7.02)	1.01 (0.815)	161 (17.89) (1.23)	1.07 (0.622)
	One member	9518	615 (6.46)	1.02 (0.729)	127 (20.65) (1.33)	1.20 (0.252)
HOURS AWAY FROM HOME ON WEEKDAYS	None	917	50 (5.45)	ref	10 (20.00) (1.09)	ref
	Less than 1 hour	1650	98 (5.94)	1.18 (0.418)	10 (20.00) (0.61)	0.57 (0.367)
	1 to less than 3 hours	7849	460 (5.86)	1.43 (0.050)	70 (15.22) (0.90)	0.75 (0.592)
	3 to less than 5 hours	5783	380 (6.58)	1.56 (0.016)	49 (12.89) (0.85)	0.63 (0.384)
	5 to less than 7 hours	3576	300 (8.39)	1.72 (0.004)	66 (22.00) (1.85)	2.04 (0.187)
	7 or more hours	15160	1271 (8.38)	1.45 (0.038)	250 (19.67) (1.65)	1.40 (0.524)
TENURE TYPE	Owner-occupier	22664	1599 (7.06)	ref	260 (16.26) (1.15)	ref
	Social rented sector	5707	365 (6.40)	0.97 (0.692)	91 (24.93) (1.59)	2.53 (<0.001)
	Private rented sector	6698	600 (8.96)	1.05 (0.464)	104 (17.33) (1.55)	1.11 (0.552)
OCCUPATION CODING	Managerial and professional	13553	1254 (9.25)	ref	237 (18.90) (1.75)	ref
	Intermediate	8081	572 (7.08)	0.78 (<0.001)	94 (16.43) (1.16)	0.72 (0.045)
	Routine and manual	11276	616 (5.46)	0.56 (<0.001)	116 (18.83) (1.03)	0.87 (0.399)
	Never worked and long term unemployed	1085	33 (3.04)	0.21 (<0.001)	6 (18.18) (0.55)	1.92 (0.228)

	Full time student	1074	89 (8.29)	0.54 (<0.001)	2 (2.25) (0.19)	0.03 (<0.001)
GENERAL HEALTH	Very good	11692	874 (7.48)	ref	141 (16.13) (1.21)	ref
	Good	14997	1037 (6.91)	1.01 (0.903)	165 (15.91) (1.10)	0.92 (0.601)
	Fair	6027	419 (6.95)	1.20 (0.040)	92 (21.96) (1.53)	1.22 (0.347)
	Poor	1904	194 (10.19)	1.74 (<0.001)	57 (29.38) (2.99)	1.56 (0.115)
	Very poor	429	36 (8.39)	1.32 (0.203)	0 (0.00) (0.00)	1.00 (-)
HEALTH CONDITIONS	Sensory conditions	1739	107 (6.15)	0.74 (0.012)	13 (12.15) (0.75)	0.38 (0.006)
	Physical conditions	5863	499 (8.51)	1.35 (<0.001)	108 (21.64) (1.84)	1.26 (0.323)
	Cognitive conditions	1474	150 (10.18)	1.05 (0.679)	43 (28.67) (2.92)	1.03 (0.903)
	Mental conditions	2422	297 (12.26)	1.62 (<0.001)	70 (23.57) (2.89)	1.13 (0.546)
	Pseudo R ²			0.0366		0.1054

Table 3.2: Financial loss summary statistics and univariate analysis.

Age group	N	Victimisation resulting in financial loss: n (%)	Odds Ratio (p)
16-24	78	28 (35.90)	ref
25-44	283	110 (38.87)	1.01 (0.983)
45-64	234	98 (42.42)	1.16 (0.610)
65-74	51	19 (38.00)	1.20 (0.660)
75+	13	9 (69.23)	4.25 (0.037)

3.4 Discussion

Cybercrime victimisation was less common with older age, as would be expected, because younger demographics continue to spend more time online, increasing their exposure to online threats (Whitty, 2019). In addition, older adults are more likely to engage in online guardianship behaviours such as using anti-virus software (Ibid). People aged 75+ were most likely to experience repeat victimisation and financial loss. It might be, given that cases experienced by older people were more serious in nature (i.e. likely to involve financial loss and repeat victimisation) that they were the tip of the iceberg, and indicative of under-disclosure of cybercrime by older people to survey interviewers. Burton et al. (2022) theorise, based on existing literature, that older adults may not disclose their victimisation due to feelings of shame, embarrassment, and fear of not being taken seriously or victim blaming. Older adults may also feel reluctant to engage with the criminal justice system, which can be an unpleasant and

stressful experience sometimes consisting of repeated interrogation by officials who are perceived as blameful and unempathetic. This phenomenon is known as secondary victimisation (Cotti et al., 2004; Pemberton & Mulder, 2023). A higher likelihood of repeat victimisation and financial loss could also reflect lower awareness of scams and reporting options in a generation adopting technologies that they did not use during their working lives, and therefore greater vulnerability to further victimisation.

I found that men are more likely to experience victimisation and repeat victimisation than women. A plausible explanation is that men, who have been found to take more risks than women generally (Hudgens & Fatkin, 1985), may also engage in riskier behaviour or activities online, leaving them more vulnerable to malicious actors. Notten & Nikken (2016) have found this to be true in the context of adolescents, who may voluntarily engage in risky or inappropriate online communications, such as disclosure of identifiers to strangers and sending photographs. This ties in with Victim Precipitation theory, which proposes that victims actually contribute to the criminal event that has harmed them, either through facilitation or provocation. Victim facilitation refers to situations where the victim inadvertently creates opportunities for the crime to occur (Lasky, 2019). It is also plausible that women underreported their victimisation in the survey due to feelings of shame to a greater extent than men. Research indicates that women may have a higher propensity for feelings of guilt and shame than men (Benetti-McQuoid & Bursik, 2005); and parallels with online scams and fraud – perhaps romance fraud in particular – can be drawn with sexual victimisation, for which shame is a significant barrier to reporting (Weiss, 2010). Women are more likely to be victims of romance fraud than men (Whitty, 2018).

Black and mixed/multiple ethnicities were more likely to be cybercrime victims than participants of White ethnicity. Research on the drivers behind ethnic disparities in crime victimisation in the UK and abroad is limited. Salisbury and Upson's crime survey analysis found that people of Black and minority ethnicity are more likely than White people to fall victim to crime in general. Future

research might explore differing patterns and types of internet use, and systemic disadvantages, for example linguistic barriers to safe cyber navigation, as well as considering the intersectionality of people with multiple vulnerabilities or minority characteristics who may need particular tailored support (Dancig-Rosenberg & Yosef, 2019).

My findings suggest a complex relationship with socioeconomic status, as those in professional and managerial occupations are more likely to experience cybercrime. A plausible explanation, consistent with LRAT, could be that professional and managerial occupations involve greater internet usage.

Worse cognitive, physical, mental and general health were associated with greater risk, across the ages. This relationship is likely to be bidirectional as poor health might increase the risk of cybercrime (Abdelhamid, 2020) and being a victim of cybercrime may worsen mental health (Rhoads, 2023). Meijwaard et al. (2015) suggest that increased crime victimisation rates among individuals with mental health disorders may be explained by the stress generation hypothesis, which proposes that individuals with depression – characterised by agitation, cynicism and irritability – experience higher rates of stressful and negative life events triggered by their own aversive behaviour. Cognitive impairment is most likely associated with victimisation due to its positive relationship with poor decision making (Boyle et al., 2012). Loneliness and social isolation, more prevalent in old age (Surkalim et al., 2022), is linked to worse cognitive function and a higher risk of developing dementia (National Institute on Aging, 2024). Crime victimisation can cause poor physical health, often through somatisation, though poor physical health as a cause of victimisation is under-researched and therefore less certain. We know that poor health is linked to social isolation (National Institute on Aging, 2019), which may be an indicator of greater internet use and therefore exposure to online threats.

Potential interventions to reduce under-reporting might include awareness-raising among police and financial institutions, and training and review of reporting procedures to ensure they are

appropriate for all age groups. There may also be scope for incorporating cybersecurity-related assistance or education into health and social care services, and increasing multiagency collaboration and information sharing with police. Staff may benefit from education and training around victimisation indicators, cybercrime reporting process and safeguarding protocol. Given that victimisation was associated with physical and cognitive impairments; software professionals might consider how online platforms and their security features and offerings can be more inclusive.

3.4.1 Limitations

I compared financial impact of cybercrime, but due to low responses to the survey questions asking about emotional and physical impacts, could not study these. There is very limited research exploring the emotional and physical impacts of cybercrime victimisation for older adults. In order to design interventions that ameliorate different forms of harm experienced as a result of cybercrime victimisation, future research might look at the comparative physical and psychological effects of different types of cybercrime victimisation across the life course. Similarly, whilst the data allowed some consideration of social isolation in terms of household size (which turned out to be positively associated with victimisation in spite of presumably more opportunities for social interaction), there were no variables that might indicate the role of social support as a mediating factor – for example attendance at social events, or availability of accessible public transport.

My research data were collected before the pandemic, and habits, behaviours and threats may have changed significantly as a result of it. Benbow et al. (2022) argue that older adults were disproportionately affected by the COVID-19 pandemic, not only in terms of the health risks but also in relation to their increased confinement and consequent loneliness and neglect. Increased use of technology by older adults during lockdowns and social distancing, and indeed during the post-pandemic era, have exposed them to new threats. Payne (2020), who found that

fraud victimisation among older adults increased from 2019 to 2020, argues that social distancing served “to displace criminal behavior from the streets into the safety of the places we live”.

3.4.2 Conclusion

Although victimisation rates were higher among younger demographics, we can confidently predict that cybercrime victimisation rates among older adults will increase over time due to increasing technology and internet uptake among this demographic (ONS, 2020) and the UK’s ageing population (ONS, 2023a). Older adults may be less able than younger adults to avoid repeat victimisation and financial loss, and may also be under-disclosing less serious victimisation (that does not involve repeat offences or financial loss) relative to younger adults in the CSEW, possibly mirroring a lower propensity to report cybercrime to the police, bank, or other authority. Future developments in platform and process design, as well as multi-agency collaboration and information sharing, should focus on empowering older adults to detect fraudulent activity before loss is incurred, and removing barriers to reporting. Whilst this study pointed towards a likelihood of underreporting, its design cannot explain why this may be the case. I used these findings to inform the topic guide for my next study, where I sought to consider the perspectives of stakeholders about how the factors identified here, including health limitations, might represent barriers to reporting cybercrime.

In Chapter 4, I present my second study: ‘Exploring the factors preventing older adults from reporting cybercrime and seeking help’.

Chapter 4: Exploring the factors preventing older adults from reporting cybercrime and seeking help: a qualitative, semi-structured interview study

4.1 Introduction

The results of my first study suggested that people aged 60+ were less likely to report cybercrime than younger people, but more likely to suffer repeat victimisation and associated financial loss. This could indicate under-reporting in older age groups, with only the most serious crimes being reported. Victimisation and repeat victimisation were also associated with poor general health and the presence of physical, mental and cognitive illnesses/conditions. Reporting crime has societal benefits and, on an individual level, facilitates access to justice, compensation and supportive services and prevents future victimisation (Tarling & Morris, 2010).

In their programme theory explaining how, why and in what circumstances older adults may be at risk of becoming victims of cybercrime, Burton et al. (2022) proposed seven factors that heighten the risk: social isolation, health vulnerabilities, memory loss, wealth, limited cyber security skills or awareness, scam content and societal attitudes. Health vulnerabilities in the form of memory loss and cognitive decline may impair judgement, decision-making capacity and ability to recall details of victimisations, whilst social isolation, more common in older age, can increase risks of under-reporting due to a lack of practical and emotional support to do so.

Rosales et al. (2023) propose that digital ageism operates on both a corporate and an interpersonal level. Corporate biases describe the under-representation of older adults within institutions that make digital technology, as well as within their design, development and testing and advertising phases. For example, digital technologies may be engineered predominantly by young professionals, unaware of the needs of older demographics. Meanwhile, interpersonal biases refer to the societal stereotypes that exist regarding age in relation to technology. For example, the idea that older adults are digital 'immigrants' and 'late adopters' rather than natives

and ‘early adopters’ fails to acknowledge that digital skills are not innate, but acquired through access, interest and practice. The portrayal of older adults as inherently digitally challenged predicates against empowerment, and provision of products appropriate to their needs, so these biases are self-perpetuating (Rosales et al., 2023). There is presently no published research exploring digital ageism within fraud and cybercrime reporting mechanisms.

This is the first known qualitative study to date to ask older victims of cybercrime, their family or professional stakeholders about their perspectives and experiences of reporting cybercrime in the UK. In view of the significant harms associated with victimisation, including the impact of digital ageism, this study asks what prevents older adults from reporting their victimisation and receiving help and support. Guided by Burton et al.’s (2022) programme theory and Rosales et al.’s (2023) interpersonal and corporate conceptual model of digital ageism, I aimed to identify the barriers that older adults face when deciding whether to report cybercrime and explore how they might be mitigated. I did this by conducting one-to-one interviews with older adults, their family members and professional stakeholders. The research was published by the journal *Health and Social Care in the Community* on 23 October 2024. The article can be found here: <https://onlinelibrary.wiley.com/doi/10.1155/2024/1314265>

4.2 Materials and Methods

4.2.1 Participants and procedures

UCL Research Ethics Committee, reference 25325/001 approved the study (Appendix 14). I advertised the opportunity to participate by distributing flyers in community venues, including local libraries, places of worship and Citizens Advice Bureau offices in one UK city, one town, and one rural ‘unitary authority area’ – purposively selected for geographical diversity across Southeast England. I publicised the study nationally on Facebook, Nextdoor, Twitter and LinkedIn, and through my existing networks with third sector organisations and health and care, and FJN professionals. I invited participants to tell others about the study. My intended sample

size was 30 participants, a moderate-to-large figure determined using information power principles (Malterud et al., 2016). I had a narrow aim, my intended participants held specific characteristics, and I expected strong and clear dialogue given I would be interviewing a combination of professionals and senior technology users – factors that increase information power and permit fewer participants. However, the study was not supported by an abundance of theoretical literature, and I was to adopt an explorative, cross-case analysis strategy – factors more suited to a larger sample size. I recruited purposively (a sampling approach in which the researcher establishes participant criteria on the basis that those criteria are necessary or at least useful for answering the research question (Bryman, 2016, p.413)): (1) People aged 60+ who reported experiencing cybercrime in the last five years, defined as online fraud or computer misuse. I included individuals who had engaged with malicious actor(s) or content over the internet. I did not include people who had received, but not engaged with phishing emails or other malicious content. I only included people with capacity to consent to take part in the research – assessed prior to the start of each interview by asking open-ended questions to check their understanding of the study – but did not explicitly exclude people with mild cognitive impairment. I developed a protocol to ensure that I took a systematic approach to managing the risk of any distress being caused to the participant during the interview, by the discussion of emotive topics. The main components of this were to maintain a compassionate, person-centred stance throughout, inviting participants to take a break or stop the interview completely; and signposting all interviewees to Victim Support UK, Age UK and police non-emergency hotlines, and giving space for interviewees to discuss any issues they wanted to at the end of interviews. As a former police officer, I am experienced in communicating with people, including vulnerable adults, in difficult situations. I retained the support of – and kept in regular contact with – CC, a consultant psychiatrist, throughout. This protocol was approved by the UCL Ethics Committee.

I purposively sought to recruit participants for diversity of ethnicity, tenure type and household size. (2) Friends and family members who had provided support to people aged 60+ who had experienced cybercrime in the last five years. They could be, but were not necessarily, the friends or family members of the people aged 60+ I interviewed. (3) Professional Stakeholders, whose professional role included supporting, in a frontline or management role, older people experiencing cybercrime. I purposively recruited professionals from policing, bank, health and social care and third sector organisations. I recorded participants' sociodemographic characteristics, and role characteristics for professional stakeholders. My decision to recruit purposively was made to obtain highly detailed and relevant insight from the specific demographics and professional fields that I had identified as being of particular pertinence to this study and its aims (Palinkas et al., 2015).

In advance of the interviews, I sent all interested potential participants a Participant Information Sheet (Appendices 1-3) and a consent form (Appendix 4) and gave them the opportunity to ask any questions. If they agreed to take part, I arranged a date and time for the interview to take place, and at the beginning of each interview recording, participants were asked to provide their consent verbally in accordance with the consent form. All participants were offered a £30 Love2Shop voucher as a token of thanks for their time involved in participating.

Qualitative interviews followed semi-structured topic guides (Appendices 5-7). I opted for semi-structured interviews because they enable the participant to express, in their own time, their unique experiences, reflections and feelings in depth whilst maintaining a degree of focus on the research question. Semi-structured interviews allow the researcher to guide the conversation through unexpected yet pertinent topics without significant restriction (Adams 2015), respecting the fact that this is a sensitive topic. My topic guides were informed by Taherdoost's (2022) guide to interview design: in order to set the scene and provide context to the answers that would follow, topic guides for all categories of participant started with broad, open-ended questions

about cybercrime in general and how one would report cybercrime. For professionals, I asked how their organisation has dealings with cybercrime victims. My questioning would then narrow in order to address the research aim whilst retaining a natural flow; asking about lived experiences, what decisions they made, what challenges they might have faced, and whether they would do anything differently if in the same situation again. I intended for participants to speak freely about their experiences, though I developed the topic guides to include multiple prompts and follow up questions in order to encourage elaboration and also to re-focus the conversation where appropriate. I used simple English and avoided jargon in order to make the questions accessible and appropriate for all participants.

People with personal experiences of cybercrime were asked about their experiences of victimisation and reporting, and decisions around reporting. They were asked discrete choice questions regarding the financial and emotional impact of their victimisations, whether they considered these to be: minor, moderate, or significant, and if financial losses had been recovered. Friends and family were asked about the support they gave during victimisation; and professional stakeholders about their experiences of cybercrime victimisations of older adults, and views on existing reporting mechanisms. Interviews were by video-call on Microsoft Teams or in-person in the participants' homes (though any mutually convenient private or public location was offered), at the participant's preference, and lasted 30-60 minutes. Recognising that the topic might be difficult to talk about, I took care to ensure they were relaxed and conversational in nature. Arguably, more of a rapport was developed during the in-person interviews, possibly owing to the opportunity for extended small talk beforehand. This resulted in a less formal and more open discussion. The older adult I interviewed in-person did, however, admit feeling some initial apprehension at the idea of meeting a 'stranger' face to face to talk about their online activity. Though many expressed lingering anger and frustration about their experiences, none of the older adults interviewed became visibly upset. Interviews were all

conducted, audio/video-recorded and transcribed by me, a mixed-methods researcher with semi-structured interview experience and a background in policing.

4.2.2 Analysis

I conducted a Reflexive Thematic Analysis (RTA) using NVivo 14 to code interview transcripts. RTA refers to the processes of critical reflection and refinement pursued by the researcher, during which subjectivity and nuance are considered in relation to predominant assumptions and socio-cultural context (Braun and Clarke 2021). Reflexivity in this study manifested as iterative examination, adaptation and refinement of themes, initially generated by me, with my supervisors. With backgrounds encompassing crime science and policing (KT), old age psychiatry (CC), and applied mental health research (AB), we purposely challenged each other's interpretations and assumptions during discussion of the data, with each of us offering different contextualisation to my findings in accordance with our respective areas of expertise. As a former police officer, I was conscious that I held a predominantly law enforcement-based perspective, which could have led me to emphasise structural and procedural barriers to reporting, such as difficulties navigating reporting mechanisms or lack of institutional responsiveness. However, through iterative engagement with the data and with my colleagues, I recognised the significant impact of psychological and social barriers, such as shame, self-blame, and fear of judgment, which I had perhaps not considered to the same degree. In conducting interviews, I was mindful of power dynamics, particularly when engaging with older adult participants who may have viewed me as an authority figure due to my research affiliation and background in the police (Finlay, 2002). Whilst I positioned myself as an independent researcher rather than someone linked to law enforcement or victim services, I recognised that my perceived institutional alignment might hinder participants' willingness to discuss their full range of experiences and emotions due to the possibility of me perceiving them in a negative light. To mitigate this, I adopted a conversational interview style, allowing participants to narrate their experiences in their own terms, and reinforced that my role was not to evaluate but to understand their

perspectives (Dodgson, 2019). Subjectivity was approached with open dialogue in meetings, and my themes and descriptions reflect a collaborative interpretation of the interview data drawn from interconnecting whilst distinct approaches. Braun and Clarke's (2021) six phase process for RTA was used to analyse the interview data, which were coded both deductively – driven by existing theory on barriers to reporting, with particular reference to Burton et al.'s (2022) programme theory and Rosales et al.'s (2023) conceptual model of digital ageism – and inductively – acknowledging that there would be unresearched or unexpected factors at play.

Phase 1 was familiarisation with the dataset. This involved re-listening to the recordings, becoming immersed in the data, and making notes with initial ideas about the barriers to reporting cybercrime. Phase 2 was coding; working through the dataset and applying labels to segments of text that appeared potentially relevant or meaningful to the research question. Phase 3 was generating initial themes, clustering codes into broader patterns and ideas, at this stage, a sample of the interview transcripts was shared and discussed by CC, AB and KT, to consider emerging themes. Phase 4 was developing and reviewing themes, whereby themes are re-assessed and compared with other themes and against the entire dataset. Phase 5 was refining, defining and naming themes. As well as breaking my data down into codes and themes, NVivo enabled me to separate these codes and themes according to participant category in order to consider the differences in results between professional stakeholders, victims and their friends and family. The final phase, 6, was the writing up.

4.3 Results

4.3.1 Sample Description

I interviewed 33 participants between August 2023 and January 2024, 31 via video-call and two in-person. 16 participants were older adults who had experienced cybercrime, two were family members (a daughter and a partner) of people who had experienced cybercrime, and 15 were stakeholders with professional, and in several cases also family experience of cybercrime. I

interviewed 18 male and 15 female participants; and people of White ($n=25$), Asian ($n=4$), Black ($n=1$), Mixed/Multiple ($n=1$), and Other ($n=1$) ethnicities, with one declining to provide information about their ethnicity. Professional stakeholder participants worked in healthcare ($n=5$), law enforcement ($n=5$), third sector support organisations ($n=2$), banking ($n=2$) and IT ($n=1$). Table 4.1 shows professional stakeholder sample characteristics.

Table 4.1: Professional stakeholder sample characteristics

Ethnicity	Gender	Sector
White	Male	Charity
White	Male	Law Enforcement
White	Female	Health and Social Care
White	Male	Health and Social Care
White	Female	Health and Social Care
White	Male	Charity
White	Male	Health and Social Care
White	Female	Health and Social Care
White	Male	Information Technology
Mixed and/or multiple	Male	Law Enforcement
Asian British	Male	Banking
Declined to say	Male	Law Enforcement
White	Male	Law Enforcement
White	Female	Law Enforcement
White	Male	Banking

Older adult participants ($n=16$) were aged between 62 and 79 years, with a mean age of 71. Most lived with a partner ($n=9$), four lived alone, and one each with their son, partner and mother-in-law, and a co-tenant. One lived in private rented accommodation, others in privately-owned accommodation. Participants used a mobile phone ($n=7$) or computer ($n=9$) to access the internet. Half ($n=8$) had a post-graduate degree; others a bachelor's degree ($n=3$), college ($n=3$) or secondary school ($n=2$) education. Six older adults reported no financial impact from their victimisation, two minor, two moderate and six a significant impact. Ten participants lost money, of whom six had at least partially recovered their losses. Five older adults described the emotional impact of their victimisation as minor, four moderate, and seven reported a significant impact. Table 4.2 shows the older adult sample characteristics.

No participant displayed or communicated any signs of distress during the interviews, though I did signpost several to further sources of support, solicited and unsolicited.

Table 4.2: Sample characteristics for older adults

Age	Lives with	Ethnicity	Most used device	Highest educational attainment	Financial impact	Money recovered at least partially	Emotional impact
66	Partner	White	Phone	Postgraduate	Significant	Yes	Significant
66	Partner	White	Com.	College*	Minor	Yes	Minor
75	Partner	White	Comp.	Bachelor	Moderate	Yes	Moderate
76	Partner	White	Comp.	Secondary	Significant	Yes	Significant
73	Alone	White	Comp.	Secondary	None	N/A	Minor
79	Partner	Other	Phone	Bachelor	Significant	Yes	Moderate
61	Partner	White	Comp.	Postgraduate	Moderate	Yes	Minor
73	Alone	White	Phone	Postgraduate	None	N/A	Minor
69	Alone	White	Phone	Postgraduate	None	N/A	Moderate
69	Partner	Asian British	Comp.	Postgraduate	None	N/A	Minor
74	Partner	Black	Comp.	Postgraduate	Significant	No	Significant
70	Partner	White	Comp.	Postgraduate	Significant	No	Significant
69	Partner & Mother in Law	Asian British	Phone	College	Minor	No	Moderate
75	Alone	White	Phone	Postgraduate	None	N/A	Significant
62	Son	White	Phone	Postgraduate	Significant	No	Significant
73	Other	White	Comp.	College	None	N/A	Significant

*'College' in the UK is a generic term typically used to describe further education institutions for pupils aged between 16 and 18 that offer specialised vocational training courses (Erfan, 2025).

4.3.2 Findings

I identified four themes, responding to my research aim (above):

Theme 1: Shame and fear of repercussion, described feelings of shame around reporting, compounded by victim self-blame for relinquishing funds or device control, and a *modus operandi* (MO) and anonymity of malicious actors that evoked feelings of guilt in victims as well as fear of repercussions.

Theme 2: Reporting perceived as unhelpful to emotional or financial recovery: Several older adults described negative effects of the scam on their wellbeing, and fear that reporting may extend or worsen their distress. This reluctance to expose victimisations further was also reflected in accounts of denial during and after victimisations. Other participants anticipated more negative than positive consequences of reporting – that they would not be heard, might be blamed and resources would not be recovered.

Theme 3: Lack of knowledge of scams and sources of support: lack of awareness of the types of cybercrime or recourse to inclusive, accessible reporting mechanisms increased vulnerability.

Theme 4: Social support helps with reporting and recovery: Professional stakeholders discussed their experiences of supportive groups or professional relationships, which could reassure victims that they were not alone, cybercrime was common, and they could seek advice if targeted in future, before disclosing information to potential offenders.

I discuss these themes in depth below using participant quotes to illustrate the themes. Participant names have been replaced with pseudonyms.

4.3.2.1 Shame and fear of repercussion

Many of the older participants described feeling too ashamed to disclose their victimisation to friends, family or the authorities for fear of how they might be perceived or what would happen as a result, often emphasising their own agency in accounts of their victimisation. An awareness of, and reluctance to fulfil ageist stereotypes surrounding gullibility, technological and general cognitive capability, also prevented reporting.

Mike, a 75-year-old male who received a text from a scammer posing as one of his children requesting money, was reluctant to disclose his victimisation to his family because it would have reflected negatively on him:

Mike: *You know it wasn't a large amount of money (...) but I felt so stupid. That's what bothered me most about it. I didn't tell [my son] all the details actually 'cause that would have made me look extremely stupid in front of him, so I didn't do that.*

Jas, a 62-year-old female investment scam victim, was one of several participants who expressed feelings of shame or embarrassment.

Jas: *They [the bank] gave me five warnings and I just didn't take any 'cause I was so confident that this was a legitimate website. It was just so convincing, and of course I'd hardly told anyone because of the shame. Basically, I was so ashamed to be so gullible to have lost £20,000, and that was it. I've got no more money. The whole lot in my bank was all gone and the sad thing is, the only reason I did it in the first place was because I wanted to clear another debt.*

The effect of negative societal attitudes around ageing on victim self-esteem was evident from one participant's experiences. Rebekah, a 73-year-old female who was persuaded to grant a malicious actor remote access to her device, recalled feeling demoralised by a friend telling her "You're not 80!", indicating an implicit ageist assumption that cybercrime victimisation of older people is related to reduced technological skills or impaired judgement.

Several participants blamed themselves for their victimisation, conveying frustration and regret for having been gullible enough, or expressing a sense of accountability undeserving of help or goodwill. Anita, a 74-year-old female who lost over £10,000 over several years in an investment scam, chose not to disclose full details of it to her family or the bank because she felt culpable - as if she was a co-conspirator in her own victimisation. This was exacerbated by a letter from her bank saying that her account had been suspended.

Anita: *I find it very difficult to talk about it. I'm a very private person anyway, which doesn't help. [My family] have no idea of any of this that happened. They know I've been*

scammed, but they don't know to what extent.

BH: *Why do you find it so difficult to talk about?*

Anita: *I think because you're criminalised. You feel like a criminal. You're made to feel like you're criminal, and you're working with these people that are criminals. And in my family, you know, that's a big no-no. [Now that they are aware,] they just can't understand how. 'Mummy, how could you have done that'?*

A number of professional stakeholders described how malicious actors sought to evoke feelings of guilt and responsibility in victims. Old Age psychiatrist Alice described how some of her patients were subjected to SMiShing scams from individuals purporting to be from the authorities, and threatening arrest unless 'debts' were paid. The term SMiShing is an adaptation of the term 'phishing' and describes the use of text – or 'SMS' (Short Message Service) – messages to deceive prospective victims into clicking on malicious links and/or giving up sensitive information (Waugh, 2024).

Alice: *We did have a few patients in the last year or two who kept getting these text messages claiming to be from HMRC [His Majesty's Revenue and Customs] saying 'You owe money, and someone's going to come and arrest you if you don't call us and pay this money immediately'. I can certainly think of a couple of patients who received these messages. I think I even received one and you know – we know just to discard them, but unfortunately I think with those two patients, although they were distressed and very anxious about it, they spoke with us before calling so they knew they didn't need to call the number, that it was a scam and that it wasn't something to worry about. But it did make me worry about other people who weren't in contact with a team like ours who didn't have someone to sort of share that with.*

Recovery service manager Simon described how an older, male patient was blackmailed by an online actor threatening to publicise his browsing history, which included pornographic material.

Simon: *There's one case that I'm particularly remembering where it was a gentleman who had been contacted. It was one of these things where he was told that they were aware that he'd been watching pornographic material online, and that they were going to let other people know. A sort of blackmailing. I was aware that this was happening, and this was one of the reasons that he came to our services some time ago, three or four years ago. I think he did receive support from the police about it, but it was one of our colleagues in the Community mental health team who was primarily giving him support with this; one of our community mental health nurses. We were indirectly involved because we were helping to manage his anxiety. That particular breakdown in his health was associated with the events that took place around that. I think he reported it to my colleague first. I'm pretty sure he was reluctant to get the police involved, but they [the nurse] decided that it was necessary.*

Both Alice and Simon's examples also demonstrate the important role health and social care professionals can have in supporting cybercrime victims to report their victimisation and begin the path to recovery, a theme discussed further in 4.3.2.4.

Two participants described refraining from reporting because of anxieties about retribution. Jennifer, a 73-year-old female who was recently widowed, described fondness for, and dependency on, her scammer. Jennifer stated that she was "sorry in general" after discovering it was a scam but elected to only discontinue their conversations rather than file a report, in part for fear of reprisals.

Jennifer: *I was sorry in general that it was a scam. (...) I had a vague concern about repercussions. Yeah, obviously I don't know much about these guys apart from what I've seen on the TV, but I'm pretty sure they're well organised criminal gangs. Yeah, and I just didn't want to sort of put my head above the parapet with that one. I just, you know, considered myself. I did think about reporting it to the dating site, but I thought better of it. Well, better or worse of it. I suppose it's sort of laziness on my part, but I'd try very much*

to keep under the parapet. (...) I suppose it was a combination of cowardice and laziness.

Yeah, but no, I just let it go.

For Bill, a 61-year-old male victim who was sold a counterfeit product online, the lack of knowledge of the scammer's whereabouts or identity compounded a fear of repercussions:

Bill: I was probably kind of creating some scenarios in my mind, that were probably a little bit absurd, about, you know, sending the boys round or whatever – you know, they've got my address. They know where I live. If I get the police involved, is that gonna cause me problems? (...) I was a bit nervous, was a bit cautious, you know, around reporting it. And the idea that a little gang would turn up in a van outside the house and chuck bricks through the window. I mean that did kind of occur to me and it did affect my decision and looking back on it, that was probably a bit absurd, but it was something that went through my mind at the time. (...) In my mind at that point I was kind of creating a scenario where, you know, I'm dealing with criminals here. (...) I mean, [the offender] could be somebody's granny or it could be a kind of Midlands hub of a Chinese gang. I mean, I just don't know and so I was discomforted at the idea of taking it further, just because of the potential implications. And you know, I've got to recognise the value of what we were dealing with here. I'd prefer not to lose 60 quid, but I can afford to lose 60 quid.

BH: So you thought that by involving the police in some way, the offenders might potentially try to take some sort of revenge?

Bill: Oh yeah, absolutely. That was probably the more kind of extreme ends of my thinking, but that's certainly played on my mind, yeah.

4.3.2.2 Reporting perceived as unhelpful to emotional or financial recovery

Several older adults referenced the negative impact of the scam on their wellbeing, and a fear that reporting may extend this, leading to more negative than positive consequences of reporting.

Others simply did not want to involve themselves in the matter for any longer.

Jas, a 62-year-old female investment scam victim described a reluctance to acknowledge, then to report, her victimisation. She recalled repeatedly ignoring alerts regarding her outgoing transactions, then feeling that she could not file a report to the bank because she had missed her chance to do so.

Jas: I just let it go. I just had to draw a line under it because it was so distressing to think, oh, that was my last little bit of money that I tucked away. I just lost, you know. It's not like I was missing out on fantastic holidays or going to splurge on a fast car. This was to cancel out a debt. There was nothing they [the bank] could do and it's not like they hadn't warned me. They had warned me. They'd warned me four times because I passed this amount of money over to them [the offender] in 2000 pound increments. You know, every time I sent it – and it was to this foreign bank – I was so confident, and I just ignored it [the warnings]. So it's not their [the bank's] fault, you know. I wouldn't give it back to me if I was a bank, you know! What a stupid thing to do. (...) And by the time my friends talked some sense into me and told me yes, it is definitely a scam, it was sort of gone, and done and dusted. And also I think every time I thought about it I just used to get really upset, then dwell on it, because there's nothing I could do. I'm never gonna get that money back.

Meanwhile, Kim, a 75-year-old female romance scam victim described wanting to end the emotional trauma from her victimisation as quickly as possible, by not reporting it.

Kim: I just wanted out, you know, to just get away, yeah. But now I feel different. I maybe should have taken more action to ensure that it didn't happen to anybody else. But at the time, I was too busy dealing with myself, really.

Anita felt that her bank wouldn't care about her victimisation or do anything to support her: "There isn't any point in reporting because nothing is going to come out of it, nobody's going to listen to you." Similarly, 69-year-old female Zara, who did not receive goods she had paid for on

an illegitimate website, felt that she would be more likely to receive “a big lecture” from the police than any form justice.

Zara: Well, at the moment the way things are going, you would never be able to get hold of the police in time. I don't think I would get anywhere with the police, and the police will probably just say, look, you should have been aware of this, and you should have been, you know, doing this and you should have been doing that. But I don't want a big lecture. I want somebody to take action. The way things have been going at the moment, I think I've lost confidence in the police.

Zara may not have been entirely wrong in her expectation of disappointment; Blake, a cybercrime protection specialist at a provincial UK police force, accepted that not all offences are investigated, citing resourcing issues and difficulties pursuing foreign, nameless, cyber criminals.

Blake: There's a finite amount of investigations that we can do, especially with what little staff we have. We have two detectives covering [n] million people, which is just insane, so obviously a lot of the cases come down to 'Protect' [a victim support element of their offering] 'cause even if we did have the investigative capacity, when the threat actor's based abroad and we've got no name suspects, and obviously, the best resource for the public is to have protective advice. (...) I don't think I've ever had a complaint about the response we give. I think generally the only complaints we get are people asking, 'why isn't this being investigated?'. Because they won't realise that we have dozens of cases just like theirs. Every single week, we've nameless threat actors based abroad, which, you know, we've got no jurisdiction over. There's been a few people in our feedback surveys that have left quite snorty reviews saying, 'I don't know why I bothered to even report it, because there's no investigation'. I understand, you know, because no one wants to be the victim of crime. And you know, if I was the victim of crime, I would want all the

resources in the world to go tackle it, but unfortunately we live in a difficult situation, so we have to make very difficult decisions, and I think communicating that to the public is often quite difficult.

One expert stakeholder suggested that awareness of resourcing issues might discourage older adults from reporting their victimisation. NHS Clinical Psychologist Katherine drew a parallel with the healthcare sector, perceiving the older generation as not reporting cybercrime for fear, as described in the healthcare sector, of using up finite resources.

Katherine: I think what's relevant here is that it might deter older people from reporting if they feel that, you know, there's a very finite resource and they don't want to take any of it up. So I think there's maybe something about education around that around saying, 'we want to hear from you'. You know, 'you're not being a bother'. You're not wasting resources. This is exactly what we're here for.

The older adults I interviewed that tried to report their victimisation often did so by phone. Many interviewees described negative experiences of telephone reporting, including long waiting times, and the need to repeat information to multiple different staff. Maurice, a 70-year-old victim of fraud by false representation struggled for this reason:

Maurice: I phoned the NatWest fraud team to report a fraud, and quite frankly, the initial response, it was horrific. It took well over an hour to even get an answer from the fraud team. When I explained that I had a serious issue, they said, 'oh, this is too big for us, we'll transfer you to somebody else'. And in doing so, they dropped the call. So I had to call again and start the process all over again. I have probably made more than a dozen calls to NatWest, and on each occasion it has taken a minimum of 30 minutes to get through to the fraud team, and on each occasion they've said, 'oh, we have to transfer you to somebody further up the line. And on a number of occasions they have immediately dropped the call. Eventually I managed to speak to what they claimed was a more senior

manager, who had a look and said, 'I can see what's happened'. The other thing that I find of concern, as I say, is that it takes an enormously long time for the calls to actually be put through to somebody and you keep getting recorded messages saying, 'we're ever so busy at the moment'. But if the fraud team is ever so busy at the moment, it shows they have got a hell of a lot of fraud and maybe need some more people in the team. You know, if you've just been [expletive] to the value of 30,000 pounds and you have to spend over an hour each time, then you get bounced to somebody else where you may or may not be cut off, but it may take another half hour to get an answer again. I actually think that's unacceptable.

Rebekah, a 73-year-old remote access scam victim recalled losing confidence in who she was talking to over the phone, to the extent that she challenged the bank even though she called them. Ringtones have caused her anxiety and panic attacks for several years following her victimisation: "I still have panic attacks out of the blue now [when the phone rings], several years on".

Kim also suffered a prolonged loss of confidence that prevented her from disclosing her romance scam victimisation.

Kim: At the time I was completely disillusioned with the whole thing and I didn't believe anything. But I just remember the emotion and the heartbreak and the disappointment and the feeling of betrayal and being used, and they weren't good feelings. And, you know, this is all these years later, I've dealt with it, so I can talk about it, but I don't think I could have talked about it to anybody at the time. I think it would have been too raw and I'd have been too ashamed to talk about it. And feel too stupid. You know, how can an intelligent person like me fall for that? But it's perfectly possible to fall for that sort of thing. And now I'm more worried about other people who are being tricked.

The emotional effects of victimisation can sometimes prevent any sort of rational decision-making around reporting in the first place. Stacey, a provincial police force safeguarding lead, felt that many older victims are “entrenched in denial” because of prolonged grooming, and that convincing them of the reality is “a challenging conversation”. In these cases, police were usually alerted by concerned family members. She remarked on the role of denial in investment scams:

Stacey: We used to see investment fraud really only for the elderly, because youngsters didn't get involved in it. That has changed somewhat, where people are getting sort of tempted to invest in cryptocurrency, on social media or something, but traditionally it would have been people with their pensions and they're, you know, trying to invest in diamonds, land, you know, timeshares, all of that kind of thing. And when they find out it's a fraud, they can be reluctant to accept it as well, because they're still trying to hope that that money [will produce a return on investment] ... that they were actually smarter. Because a lot of them are clever people and they've done a lot of research, and they can't accept that they've been had over in that way.

BH: How would you become aware of these incidents if they're not reporting it to you?

Stacey: So family members, neighbours, friends, carers. And as I say, other agencies, financial institutions. You know, if somebody's going into the Post Office to send money, they there they'll phone us.

4.3.2.3 Lack of knowledge of scams and sources of support

A number of participants described a lack of awareness of different types of cybercrime or reporting mechanisms. Several of the older adults interviewed were unfamiliar with Action Fraud – the UK's national reporting centre, and central point of contact, for fraud and cybercrime. When asked, Rachael, a 66-year-old female who had been the victim of a QR code scam (where the victim is directed to fraudulent websites via counterfeit QR codes) stated: “I may have [heard of it], but it doesn't come to mind”. Likewise, Alasdair, a 69-year-old male who was targeted by a

vishing scammer purporting to be a British Telecom employee, told me he'd heard of Action Fraud, but wasn't familiar with it.

When asked if she knew what cybercrime was, and how to report a scam, Heather, a 66-year-old who was victim of a fraud by false representation, had some awareness, but was unsure of different systems:

Heather: I don't understand much about [cybercrime]. You hear about it with these scams, people getting emails and texts and phone calls, trying to persuade them to click on something or send money in or give in their bank details or whatever. That's about as much as I know.

A police cybercrime protection specialist, Blake, described how unfamiliarity with cybercrime *modus operandi* increased the likelihood of victimisation, because the target is unable to identify or recognise threats:

BH: What is the general profile of the adults who fall victim to scams? What are their main vulnerabilities?

Blake: They're not necessarily low intelligence. It's more that they're not able to detect scams. So some of the most like brightest and switched on people I know, they will still fall victim to cybercrime if they don't know what to look out for. So it's difficult to pinpoint the exact vulnerability which is making people susceptible, but all I'd say is that they've just not received any kind of awareness of what kind of scams are out there before, which is why my role is so important to provide that training to people.

Former Trading Standards officer Stephen echoed these views:

Stephen: They admit they don't recognize it as a scam at the early stages. And it's not until they're part of it that maybe some of them are going to part with quite considerable sums. And of course it's not just the elderly. We find that people who have just recently retired,

who I certainly wouldn't put in the elderly bracket, are being scanned out of their pensions and their retirement investments. So it is becoming, you know, more of a problem that's got to be dealt with.

This was exemplified in the situation of Katy, who described how her 69-year-old mother experienced a postal delivery SMiShing scam, losing £3 repeatedly by clicking on a fraudulent link before her daughter explained that this was a type of cybercrime.

Katy: In my mum's case and my dad's case, they feel quite scared that they'll click the wrong link, or that they'll input their card details wrong. And so it will be largely up to me to do the bookings for them or sort out what they're ordering for them. When I was living at home, I ordered something to come through the post and my mum received a [non-legitimate] DPD text related to a package being delivered, and so she automatically assumed that this was my package, and that the text was being sent to her phone so that she was able to track where it was at. But then she ended up being scammed out of £3.00 every time you click the link. So I spoke to her after that (...), advising what these sorts of [fraudulent] links look like.

Unawareness of scams and reporting options can be caused or exacerbated by cognitive impairment, too. Leo, a clinical nurse specialist for an NHS memory service, commented on the vulnerability of individuals with memory loss to cybercrime, as they were unable to retain information about the risks:

Leo: We offer some basic information about how to manage online, and things like that. Without being unkind to the people that we work with, that information is in one ear and out of the other, because that information is just not retained in any way, shape or form. If we offer any sort of paper advice, you know, like Age UK have got some really good stuff about scams online, the chances are they would probably read it and forget it. Or never read it or, you know, they'll lose where this information is. It's really difficult to be honest.

I think, the thing is, they're not the type of people who would go into dodgy websites, that sort of thing. I don't think so. They would more likely be scammed by something sort of masking themselves as a legitimate company that they would get involved with. You know, a bank or some kind of utility or something like that.

He goes on to remark on different scam victimisation risk categories among people with dementia:

Leo: If you think about dementia from the point of view of three different sorts of categories or progression, 'mild' being people who are newly diagnosed, probably still functioning, you know, at a very, very high level – still driving, going on holidays, still doing a lot of their own day-to-day business, you know? I mean like banking and all the rest of it. And then there's 'mild to moderate'. So this is people who are obviously deteriorating a little bit and so mild to moderate are the people who are most at risk, I think of any form of scam. And then the people who, because of their cognition being so impaired, they would probably not even answer the telephone, to be honest. They probably wouldn't open the door to anybody, you know.

NHS general practitioner Charlotte commented that the burden of any sort of ill-health can affect one's capacity to acquire new technological skills or knowledge, and that older adults are often less familiar with technology relative to younger people. She also remarked on how there is a generational disadvantage for older adults, who were not surrounded by digital devices during their youth.

Charlotte: I look after all sorts of people, all aged. But yeah, I have elderly patients who are definitely vulnerable to cybercrime. They are elderly, living alone usually, although not always. They're elderly and vulnerable, usually through ill-health or poverty. One man I'm thinking about is blind, so, you know, that just makes everything more difficult, doesn't it? You know, reading, understanding things. I feel like, when you have like a large burden of

ill health, you just have a lot on your mind. You have a lot going on. You know, getting yourself kitted out IT-wise is not your priority. Plus these people, you know, the elderly, are really, really disadvantaged when it comes to IT because they've not grown up with it. And I think they don't understand it. And you know, they're not tech savvy at all. One of the patients I had, he was being bombarded with lots of stuff in the mail that was just sort of dodgy; catalogue scams and those types of things. He'd sort of say sometimes, 'can you open my post or look at my post' and he would have tonnes of post. He was being bombarded with stuff in the mail and then a couple of times the phone would ring when I was visiting him at home, because he couldn't get out because he was blind, and also he had loads of problems with his feet and couldn't walk properly. And then the phone would ring, and I could tell it was a scam call. And he's just not understanding that it's a scam call. And I'm thinking, 'god, just tell them to get lost, you know, hang up the phone'. And he's confused by it.

Additionally, 66-year-old romance scam victim Heather suggested that older adults might feel overwhelmed or condescended by the abundance of scam-related advice and information given out, which could be antagonistic rather than helpful.

Heather: All the banks and things always have long lists of 'don't do this' and 'don't do that' and 'we'll never ask for your password on the phone' and things like that, and I remember going into Lloyds Bank and I needed to take out quite a lot of money. I had to go through a whole long list of questions, including 'is there somebody waiting around the corner that you've got to give this money to?' And I was quite happy to answer those questions 'cause I knew that they were asking for very sensible reasons because there's been so much scamming and frauding and people being coerced into going into their banks to take lots of money out. And she said, 'oh, I'm so grateful that you've answered all these questions without getting cross', and that 'most people, when asked these

questions, they get cross with me and say, 'well of course they haven't'. Of course I haven't done that." Which is difficult for the bank employees because they're trying to protect people and their money from scams and things. Especially if you want to take out cash, quite a lot of cash, it's almost like you have to justify why you're taking out your own money. But I can see why. I think that's the trouble. Older people feel patronised, but they're asking these questions of everybody, not just older people. But I think older people probably get a bit irritated.

Finally, several professional stakeholders perceived older adults as being less likely to distrust, and more likely to engage with, unsolicited communications. NHS (National Health Service) Clinical Psychologist Katherine suggested that older age groups might feel compelled to respond to seemingly legitimate approaches by illegitimate fraudsters.

Katherine: I think it's probably generational. So maybe the kind of younger older people now are less likely to, but certainly the older, older people that I worked with would never have questioned a doctor, for example. You know, if a doctor says something, you do it. Or you know that if somebody calls you and they tell you they're from the bank, you wouldn't dream of not answering the phone, for example. If I think about how I might respond to an unknown message, I just wouldn't. And I think with some of the older people I've worked with, there's more of a sense of doing things properly and of being deferent to people in positions of authority. So I think that makes them more vulnerable.

4.3.2.4 Social support helps with reporting and recovery

A number of professional stakeholders highlighted the positive effects of social support, in particular formal or informal group 'sessions' for older adults in community spaces, as a means of imparting practical advice and key messages, raising awareness, and providing older adults with the opportunity to share their experiences or concerns with peers and trusted professionals. Anthony, an IT professional specialising in providing computer help and support in his

community, commented on how messages emphasising the commonness of cybercrime victimisation, or in other words ‘conventionalising’ it, enables older adults to open up.

Anthony: [It’s] useful to say, look, you’re not alone. You’re not the first. If you’re getting scammed, it’s something that’s going to happen to a lot of us, probably. So yeah, it’s making them not feel isolated.

Perhaps through increasing understanding that cybercrime is common, and that victims are not alone, Aaron, a digital inclusion coordinator of a charity for older adults, described the positive difference that group scam awareness sessions in community centres, libraries and sheltered housing can make:

Aaron: I’ve just put in two bids for Nintendo Switches. We’ve got two day centres, so I want to do gaming sessions for the older people that are at the day centre. So that’s one of the digital inclusion aspects we want to do. The cybersecurity and scam awareness sessions outside of the gaming are incredibly popular I think. We do have quite a good turnout to these sessions when we run them online and we also run them in person on occasion too.

BH: Why do you think they’re so popular?

Aaron: I think because the media highlights scams quite a lot, especially over COVID as well. I think there was like a new awareness of what’s coming in through technology, and I think there was lots of stories over COVID about older people being targeted quite a lot.

Kieron, a Police and Crime Commissioner representative, commented on how such sessions not only address important public agendas such as loneliness and ill-health, but they also represent educational, intelligence-gathering, and crime disclosure opportunities too.

Kieron: People who bring all the people together in a community place in centres or whatever, to have cakes, listen to music, have tea and stuff, can be really profound for a number of different public health agendas. Now, Loneliness was a massive problem before COVID and it’s much worse now. The simplicity of somebody making the effort to coordinate the space and advertise it locally and get all the people, encourage them to

come and then create a community. I've seen it in a couple of places and it's really, really powerful in terms of direct health benefits, literally less A&E and health problems being spotted, all that stuff, and it just feels like a brilliant way to convene the audience that you want to convene to educate. And I think you'd actually uncover a lot more crime that is already happening through that as well. And putting in effort to create spaces during the week, it doesn't have to be everyday or whatever, where you really work hard to get older people to come to a place to tackle loneliness in the sense of community, and then use that as a way to tackle a number of different key social policy agendas. And this (is) one of them.

Several interviewees described how establishing trusting relationships with older adults was key to providing support to prevent future victimisation. Charlotte, an NHS general practitioner, emphasised the need for advocates to support victims of cybercrime with dementia to seek help:

Charlotte: Anyone with dementia is going to struggle, is not going to be able to report. I'm just thinking of most of my patients, you know, my vulnerable elderly patients. They've never got up to speed with tech necessarily, but they could phone. But someone with dementia is not going to phone, and if they do phone, they're not going to express themselves. So they're not going to say the right things to the person on the other end of the phone because, you know, they need an advocate to do it for them.

Psychiatrist Alice recalled how a patient only revealed their pornography related victimisation to one particular nurse who he trusted.

BH: What particular factors do you think might make older adults vulnerable to cyber-attacks?

Alice: I think that because they're not, you know, as we describe them, digitally native, and so they've not been immersed in this digital world like younger adults have. I think that they're just a lot more vulnerable. I think that using digital technology causes a lot

more anxiety in older adults. I think they feel a lot less confident. I mean, these are obviously sweeping generalisations because we can certainly think of several 90 year olds who are very, very competent at using iPads and managing everything online, but I think those are the main sort of things that I think make older adults particularly vulnerable. And I think in this patient's case, we have the added issue that shame was such a huge barrier for him. So he didn't tell us initially when we'd assessed him that this had been happening. It was only later that he was able to confide to a trusted nurse, who I think it helped that that nurse was male as well. I think he felt more able to share that information than perhaps he would have been with a female member of staff. (...) But it did make me worry about other people who weren't in contact with a team like ours who didn't have someone to sort of share that with.

Similarly, Charity worker Aaron suggested that victims could overcome their fear of negative perception by talking to someone neutral, who they trust not to make judgements.

Aaron: I think an organisation like Age UK provides a layer of trust. Because often it's the nerves. I think clients can be a bit nervous to act on something. When they're not sure if it's a scam or not, I think there's a nervousness that they're gonna come off looking silly, basically, so having someone a bit neutral I think is what benefits them as a first step.

Several of the professional stakeholders interviewed referred to the importance of victims being able to open up and discuss their victimisation with others for emotional recovery. Recalling one example with a client, IT help professional Anthony remarked on the psychological benefits of dialogue and informal counselling around scam victimisation:

Anthony: She seemed embarrassed to talk about it to me. But on the other hand, she was glad. In fact, me visiting her helped her to rationalise it, deal with it. So there's a bit of psychology where I think she enjoyed telling the story. It was a bit cathartic to help her to get over it a bit, I felt that she wanted to tell me the whole story. So I sat there for about... it probably took about half an hour to relay the whole story to me. So I actually did a bit of

counselling in a way which it does happen actually in in my role. A bit of listening and a bit of empathising really, saying, yeah, you've done the right thing. Don't feel embarrassed about it. Going back years ago, I used to think, 'God, how can people fall for it?' But now I've seen how seeing so many people that have been caught... my attitude now is much more reassuring. Supportive. 'You've done the right thing. Let's deal with it' sort of thing. I've certainly seen more of it in the last year or so, certainly had two to three in the last year. They'd like someone to talk to, somebody they can trust. So I've built quite a trust and rapport with a lot of people and advising them and yeah, giving them ideas of how to how to stay safe online. In fact, I'm starting a newsletter. I've done one so far. I was trying to do it monthly just to sort of give them the current thread of threats. What's going on about sort of like the Amazon scams, the YouTube scams, Facebook scams, that sort of thing, and that that's that went down quite well actually.

Meanwhile, Deborah stated that cybercrime victims including her husband, who was targeted by an investment scammer purporting to be a close friend, would benefit from sitting down with a professional, such as a police officer, in order to “feel heard”, “otherwise the shock and the trauma sits in them, and they feel like they’re in prison”. 69-year-old online fraud victim Zara also mentioned how discussing her victimisation, and cybercrime in general, with friends or trusted professionals was informative and boosted her confidence moving forwards.

Zara: As you're getting on older, sometimes you can panic and you can take the wrong action [whilst using the internet], but it also makes you aware and you talk about it with friends as well to see if they've also had a similar experience. And nine out of ten times, most of them have had something like that happening too.

The bitterness directed at 74-year-old investment scam victim Anita by her husband demonstrates that a lack of support from family and friends can have the opposite effect, and actually reinforce feelings of shame:

Anita: *I don't think he's ever going to understand it. He really is terribly negative about it all. And I can't have a conversation with him – he just shouts if I talk about it and so the best thing is to avoid the subject as much as you can. You feel very guilty, and you keep asking questions as to why – 'why didn't I recognise this'. I don't have the answers. I want my money back.*

Jim, a crime prevention lead for a seniors' support organisation, stated that stopping and establishing the legitimacy of an approach with a trusted individual would be his single most important piece of advice to give:

Jim: *If you get a phone call out the blue, stop and think. Think logically, and if it's something that's trying to pressurise you into making a quick decision, talk to somebody else about it.*

4.4 Discussion

4.4.1 Barriers to reporting and the value of social interaction

To my knowledge, this is the first qualitative study to explore how older victims of cybercrime, family of victims, and stakeholders experience reporting their victimisation and seeking help. Consistent with Burton et al.'s (2022) programme theory, older adults described feelings of shame as a principal barrier to reporting, though none expressed concerns around losing their independence (though it may still have played a role). Besides shame, fear of retribution and perceptions of negative sequelae of reporting often outweighed perceived benefits. Professional stakeholders identified opportunities within their roles to increase their offering to older victims of cybercrime: for example, health and social care community professionals are well placed to support victims to report, especially those whose cognitive, mental or physical ill-health are significant barriers to reporting. Both professional stakeholders and older adults valued social interaction, including cybersecurity-focused local group 'sessions' for older adults hosted by trusted authorities, as ways of raising awareness and tackle ageist stereotypes. This is reflective

of social isolation and the absence of guardianship as risk factors of cybercrime victimisation, as proposed by Burton et al. (2022). Limited awareness of cybercrime modus operandi and reporting channels – also featuring in Burton et al.’s (2022) programme theory, were represented practical barriers to detection and disclosure. Health vulnerabilities and social isolation were also reflected in my data, but it was often the reactions or anticipated reactions of society to these vulnerabilities that influenced participant’s reactions to their victimisation and reporting behaviours, as discussed in 4.4.2.

4.4.2 Ageism and underreporting

Participants appeared to be describing digital ageism in the form of ‘pervasive social attitudes’ (or ‘interpersonal biases’). Older adults’ accounts of reticence to disclose victimisation, including to friends or family, reflected fear of embodying ageist societal stereotypes surrounding the gullibility and technological incompetence of older adults; they anticipated criticism and condescension. Such fear can also discourage older adults from using, and consequently benefitting from, technology (Mariano et al., 2021; Martin et al. 2023). Rosales et al.’s (2023) interpersonal and corporate conceptual model of digital ageism offers a valuable lens for interpreting these findings, highlighting how both individual and systemic ageist biases shape older adults’ digital experiences and responses to cybercrime. Interpersonal digital ageism manifests through internalised stigma and fear of judgment, which were reflected in participants’ reluctance to disclose victimisation due to embarrassment or concerns about appearing technologically incompetent. Some participants anticipated negative societal perceptions of older adults as ‘gullible’, reinforcing self-blame and discouraging reporting. At the corporate level, digital ageism was evident in participants’ experiences of unhelpful and exclusionary reporting mechanisms, such as long wait times, repeated questioning, and impersonal interactions, which created additional barriers for victims already struggling with distress.

Many of the experiences of reporting systems described by participants felt indicative of a failure to account for age-related vulnerabilities in their design. Experiences of telephone reporting, with long periods on hold and requirements to repeatedly narrate traumatic events to different operators, felt faceless, dehumanising and excluding of individuals with physical or cognitive disabilities. An abundance of scam and fraud prevention advice and alerts by the FJN, particularly banks, were not necessarily perceived as supportive, and could be overwhelming to individuals less able to retain or process information; or patronising those with more digital skills. There was a suggestion that such current systems, that were perceived as untargeted or targeted by age alone, would be more effective if tailored to customer preferences and capabilities.

Some older victims' reluctance to disclose victimisation to the authorities was derived from a perception of cybercriminals as highly organised and with considerable capacity to enact retribution. Cross and Richards' (2015) Australia-based study found that victims' understanding of fraud was heavily influenced – and often exaggerated – by television shows. They found that these programmes' depictions of special 'sting' operations resulted in unrealistically optimistic expectations of law enforcement agency capabilities. One interviewee referenced television as influencing his perception of perpetrators, suggesting media influences may have affected his reporting behaviour.

4.4.3 Limitations

Whilst not a limitation as such, it is valuable to note that the participants' stories were their personal version of their cybercrime experience, shaped by memory and perspective. Indeed, the coding process was also inherently interpretative. It is important to acknowledge researcher and participant subjectivity, and valuable to reflect on it rather than perceiving it as a threat (Braun & and Clarke, 2023).

There are a number of limitations to this study. Firstly, only older adults willing to disclose their victimisation to the researcher participated, so I could not capture the views of those most

unwilling to disclose, who may have been particularly distressed or traumatised by their experiences.

The small number of family members interviewed limits the transferability of findings relating to this group, but this data can be considered contextual. 'Transferability' is a term that refers to the drawing of information from one context and critically appraising it's applicability in others which are perhaps unstudied. It differs from generalisability, which is better suited to automatic, probability and rule-based applications (and therefore usually quantitative research) (Drisko, 2025). I planned to include family members who were care partners, where participants wanted to include family members to support them in telling their story. In practice, most participants did not need or want this. As a consequence, the family perspectives were limited.

Older adults with serious cognitive impairments were not interviewed for ethical reasons, meaning I were only able to access second-hand perspectives of their experiences from professional stakeholders. I did not include participants who were not English speaking, and for pragmatic reasons recruitment was limited to Southeast England; communities facing language barriers were not included. My sample of older adults consisted predominantly of White British nationals with a relatively high level of education. Future research could usefully explore barriers faced by minority and underserved communities, such as improving access to educational resources.

4.4.4 Conclusion

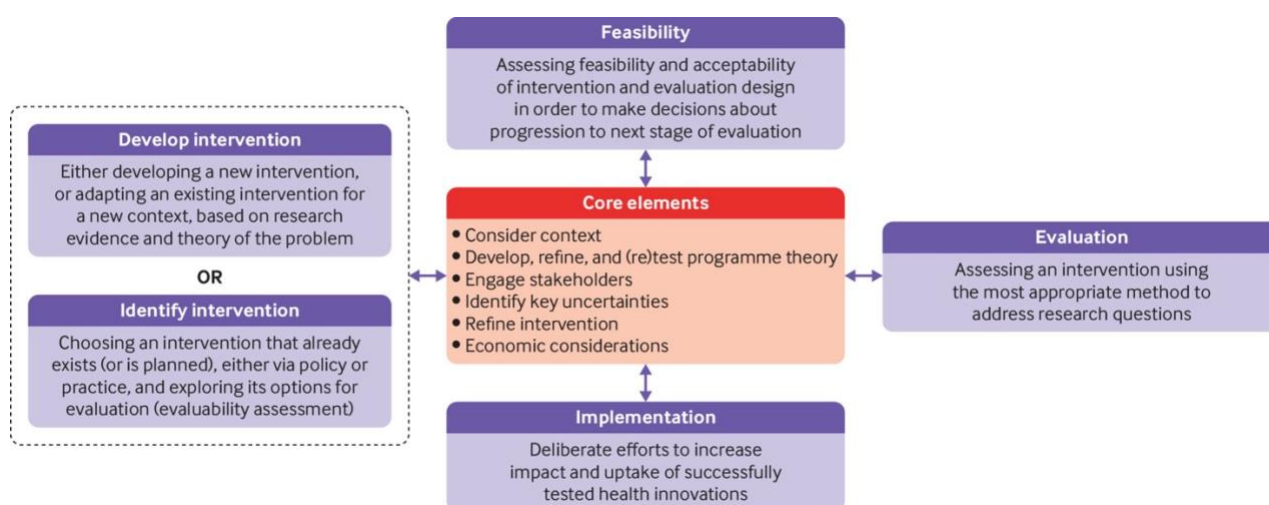
In this, second study, I uncovered a series of barriers to reporting – some of which are underpinned by interpersonal and corporate digital ageism – which serve as target areas for policy makers seeking to increase rates of disclosure. I propose that to tackle these barriers, multi-agency collaboration across health and care and justice networks is required. In chapter 5, I present my third and final study, 'Stakeholder workshops to generate intervention proposals for increased cybercrime reporting among older adults'.

Chapter 5: Stakeholder workshops to generate intervention proposals for increased cybercrime reporting among older adults

5.1 Introduction

In my third study, I conducted a series of workshops with the aim of generating intervention proposals for increased cybercrime reporting among older adults, informed by my findings from studies 1 and 2. The UK Medical Research Council (MRC) has proposed a framework for developing and evaluating complex interventions (Figure 5.1) – complex because of “the number of components involved; the range of behaviours targeted; expertise and skills required by those delivering and receiving the intervention; the number of groups, settings, or levels targeted; or the permitted level of flexibility of the intervention or its components” (Skivington et al., 2021:2). The framework consists of four phases: development or identification of the intervention; feasibility; evaluation; and implementation. The phases have a set of six common core elements that should be considered: Consider context; Develop, refine and (re)test programme theory, Engage stakeholders, Identify key uncertainties; Refine intervention; and Economic considerations. In this study I focused on the ‘develop intervention’ phase, and in doing so I incorporated two of the core elements; engage stakeholders – which I did through a series of workshops – and consider the context – which my first two studies explored. The results of which were presented to workshop participants.

Figure 5.1: MRC Developing and evaluating complex interventions framework



Rather than developing a programme theory, another core element of the MRC framework, I incorporated a Theory of Change into this study. Whereas a programme theory is the overarching model of how a particular intervention or programme is expected to work (Maden et al., 2017), a theory of change theorises how a desired ‘change’ can be brought about; a “hypothesised causal pathway to impact (...) developed in collaboration with stakeholders and modified throughout the intervention development and evaluation process” (De Silva et al., 2014:2). The desired change, in this case, would be an increase in cybercrime reporting by older adults. A Theory of Change was more suitable than a programme theory here because the intervention had not yet been developed.

5.2 Aims and objectives

The aim of this study was to capture stakeholder thoughts and ideas around potential activities or interventions that, with development and materialisation, would address the barriers to reporting I identified in my second study: (i) Shame and fear of repercussion; (ii) Reporting perceived as unhelpful to emotional or financial recovery; (iii) lack of knowledge of scams and sources of support, and (iv) Social support helps with reporting and recovery.

5.3 Methods

5.3.1 Participants

This study adopts a patient and public involvement (PPI) research approach – one which is “performed ‘with’ or ‘by’ patients and members of the public, rather than ‘to’, ‘about’, or ‘for’ them” (NIHR, 2024). PPI is valuable in the conduct and design of projects for patients or the public because it recognises the importance of lived experiences, it ensures those individuals have a say in the research that is shaping outcomes developed *for* them, and because it acknowledges their agency as active and engaged individuals rather than merely subjects (Biggane et al., 2019). I purposively sought participation from older adults aged 60 plus who used the internet or digital devices regularly, with age and gender diversity, who would be potential end-users or beneficiaries of an intervention to increase cybercrime reporting by older adults. I also sought participation from potential intervention implementers, including police officers and third sector workers who support older people; and health and social care professionals, recruited for role diversity. I held separate workshops with each of these participant groups, that is I opted for homogeneity of group given the considerable discrepancies of these stakeholder groups in expertise, experience and reference points which may have inhibited participant confidence and general conversational flow in a mixed group (Roller, 2020). Whilst retaining a level of flexibility and openness to holding more workshops if they did not yield a satisfactory quantity or quality of intervention ideas, I planned to recruit between 15 and 20 participants and to hold three to four small workshops with up to five participants in each. These would be small enough that everyone could contribute and interact together, but not so numerous that the conversation became fragmented and difficult to manage (Krueger, 2014). In deciding how many workshops to run, I was conscious that determining sample size in advance of data collection is problematic because, theoretically, new meanings and interpretations are an infinite possibility (Low, 2019). However, for practical reasons around time planning and my institutional ethics

application, I needed to estimate the number of workshops required. I considered the findings of Wutich et al. (2024), whose integrated review of literature on sample sizes indicates that four workshops is generally a sufficient number for the researcher to be able to identify a high number of meaningful themes. I opted against pursuing ‘thematic saturation’ (a term used to describe the stage in qualitative data collection when no new insights, codes or themes are yielded) given its implication that researchers are archaeologists of data rather than reflexive interpreters of data, which is therefore incompatible with reflexive thematic analysis (Braun & Clarke (2021)). I therefore remained open to the possibility of conducting more workshops if I felt that there were some important themes that I had begun to uncover which needed further exploration.

5.3.2 Procedures

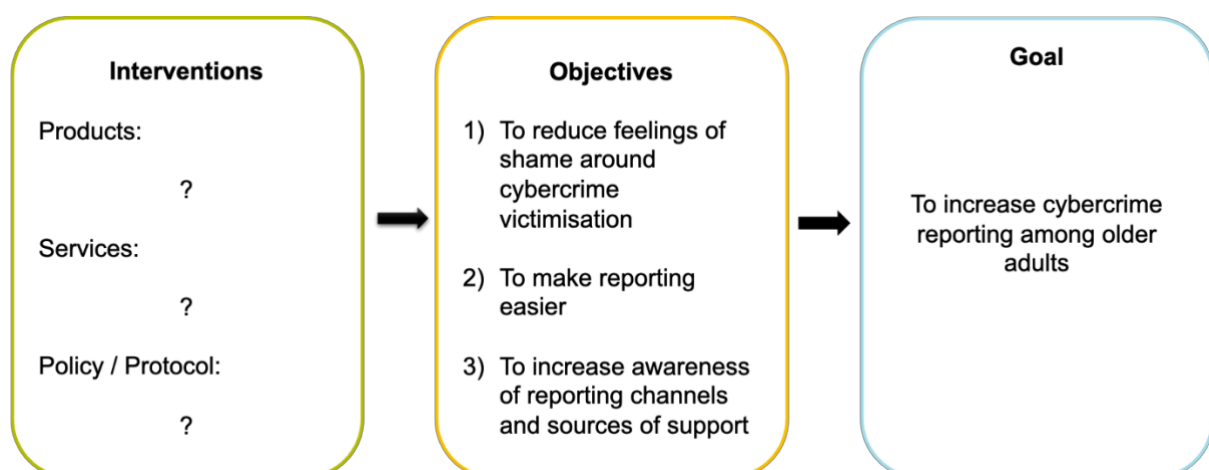
I held workshops through Microsoft Teams or Zoom, through which our conversations were transcribed automatically. Aside from negating the need for travel and related expenses, virtual workshops have been found to yield similar content to in-person methods (Guest et al., 2020; Woodyatt et al., 2016). I recruited professional stakeholders through direct solicitation on LinkedIn or their organisational website (Appendix 18: Study 3 direct solicitation message), or via email or phone to contacts already held by the research team. The opportunity for participation was publicised to older internet users on Nextdoor, LinkedIn, Facebook and Twitter (Appendix 15 – Study 3 social media publicity). Interested individuals were invited to express their interest by emailing me. Participation in study two was an exclusion criterion.

In advance of the workshops, I sent all participants a consent form (Appendix 16) and asked them to sign and return by email if they would like to take part, after reading all the information and having an opportunity to ask questions via telephone or email. I also sent them a Participant Information Sheet (Appendix 17) containing details and expectations (e.g. agenda, ground rules and roles and responsibilities) as well as an accessible summary of evidence from my previous

research and recent literature review. Participants were offered £40 as a token of thanks for the time involved in participating.

I chaired and moderated all workshops. CC and KT co-facilitated one workshop and AB co-facilitated two. All workshops lasted between 60 and 90 minutes. Dialogue was key, with “participants (...) encouraged to question each other’s responses, elicit clarification and explore caveats to their statements” (Freeman, 2006:492). I began by asking participants to introduce themselves. In workshops with older adult participants, I asked what their most used digital device was as an ice-breaker to make everyone feel more comfortable talking to the rest of the group. With all other participants I asked them their organisation and role. I then spoke about workshop expectations; that all participants have equal value and should be treated with respect, that there are no right or wrong answers, and that we take turns speaking. I then delivered a brief Microsoft PowerPoint presentation providing context and information about the current and previous studies, including Burton et al.'s (2022) exploration into how, why and in what contexts older adults are at risk of financial cybercrime victimisation. I described the goal of the workshops: to develop ideas for interventions that respond to the evidence I identified in study 2 (see goal and objectives in 5.2). Participants were encouraged to propose interventions in the form of products, services and/or policy and protocol changes.

Figure 5.2: Workshop theory of change template



I used Google Jamboard, a digital whiteboard, as a tool for interactive discussion, with participants asked to shape discussion by writing different ideas on the Jamboard and develop the theory of change as they saw appropriate, including through the suggestion of further or different intervention categories. The sessions were recorded and transcribed automatically by Microsoft Teams and I subsequently corrected the transcripts for machine error.

5.3.3 Analysis

I conducted Framework analysis of my workshop transcripts, following Gale's (2013) six stage procedure: (i) Transcription; (ii) Familiarisation; (ii) Coding; (iii) Developing a working analytical framework; (iv) Applying the analytical framework; (v) Charting data into the framework matrix; and (vi) Interpreting the data. Framework analysis was developed specifically in the context of conducting applied qualitative research by Ritchie and Spencer (1994). Framework analysis lends itself to producing actionable and auditable research outcomes given its well-defined systematic procedure and its illustrative matrix, which can be easily broken down into different themes by a range of users with differing expertise (Ritchie & Spencer, 1994). It is by its matrix which Framework analysis is defined; rows, columns and cells of data that provide a structure into which data can be summarised (Gale et al., 2013).

Having manually corrected my transcripts for machine error, I read through each of them twice, familiarising and refamiliarising myself with the data. I then began coding – applying labels to each quotation using NVivo software. My codes represented individual intervention ideas, such as 'make a video' or 'hold a training session'. I had initially intended to build my framework deductively using the theory of change model objectives that I had used in each of the four workshops as themes on one axis, and workshops on the other – with cells populated with quotations. I quickly found that the codes often bridged at least two of the three objectives I had set out in the theory of change, so inductively developed a new set of themes which I used to reorganise the coded data to check for fit. Having charted my data and themes onto the

framework, I reinterpreted my framework, finding certain commonalities and distinctions among my themes, and decided upon five new overarching themes that encompassed my 14 original (now-sub)themes.

5.4 Results

Seventeen individuals participated across four workshops on 25 June 2024, 29 June 2024, 4 July 2024 and 10 July 2024. Table 5.1 shows the sociodemographic and role characteristics of workshop participants.

Table 5.1: Sociodemographic and role characteristics of workshop participants

Workshop Number	Category of Participant	Participant Number	Gender	Role
1 (25/06/24)	Health & Social Care Professionals	1	Female	Occupational Therapist
		2	Female	Social Worker Team Lead
		3	Female	Old Age Psychiatrist
2 (28/06/24)	Other key professional stakeholders / intervention implementers	4	Female	Victim Charity Manager
		5	Female	Police Fraud Caseworker
		6	Male	Old Age Charity Digital Specialist
		7	Female	Security & Justice Advisory Firm
3 (04/07/24)	Older Adults	8	Male	Older adult aged 60 or over who uses the internet and/or digital devices on a regular basis.
		9	Female	
		10	Male	
		11	Female	
		12	Male	
		13	Female	
4 (10/07/24)	Older Adults	14	Male	
		15	Female	
		16	Male	
		17	Female	

Workshop 1 comprised three health and social care professionals with significant experience working with older adults. Workshop 2 included four potential intervention implementing partners, including representatives from a provincial police force, an Old Age charity, a crime victimisation support charity, and a private think tank and consultancy. Workshops 3 and 4

comprised 10 adults aged 60 plus (six participants in one and four participants in the next) who used digital devices and/or the internet on a regular basis.

In my framework analysis, I identified five activities (themes) and 13 activity ‘components’ (sub-themes) (Table 5.2). The matrix I developed during this analysis is in Appendix 20.

Table 5.2: Activities and activity components identified in workshops in response to the goal and objectives presented

Activity	Activity Component
Holding interactive cybersecurity sessions that bring older adults together	Creating an environment that allows older adults to feel comfortable about opening up
	Capitalising on the common desire to socialise and learn to impart cybercrime and reporting advice
	Providing educational resources with universal messaging to aid session facilitators and for attendees to take home
Engaging previous victims of cybercrime to offer support and advice in different contexts	Setting up peer support helplines for victimised or concerned older adults
	Inviting previous victims to be guest speakers at cybersecurity sessions for older adults
Engaging younger demographics and other trusted individuals in educational and supporting roles	Organising IT help schemes where younger people are matched with older adults in need of IT support
	Translating and interpreting of cybersecurity advice, cybercrime reporting processes and potentially malicious communications by younger people for older adults whose first language is not English
Communicating messages that normalise and decatastrophise victimisation	Emphasising victim faultlessness
	Maximising message impact through television and radio
	Making the most of NHS and care services to reach those in need of support
Training stakeholders on communicating empathetically and recognising victimisation signs	Using more empathetic and less victim blaming language when speaking with potential victims of cybercrime
	Upskilling stakeholders to provide sound advice and to recognise and act on signs of victimisation

5.4.1 Holding interactive cybersecurity sessions that bring older adults together

An idea stemming from all workshops was to hold cybersecurity awareness ‘sessions’ or ‘events’. Participants frequently spoke about how bringing older adults together in a safe space, either virtually or online, to learn from a legitimate and trusted authority about cybercrime and cybersecurity could be educational in terms of identifying scams and understanding reporting mechanisms, and conducive to destigmatising discussion.

5.4.1.1 *Creating an environment that allows older adults to feel comfortable about opening up*

Professionals with experience of holding cybersecurity or technology inclusion events spoke about how they provided an opportunity for attendees to share and process their own victimisation experiences, and for others to learn from that insight. One victim support charity manager remarked that attendees who have been victimised but have not reported their victimisation will, by the end of the session, often feel comfortable enough to discuss their experiences:

Over the last eight years of supporting fraud victims, both reactively and proactively when doing community engagement work, you will find a large number of people come up to you at the end of a session to say, “that did happen to me, but I haven't reported it” for reason X, Y and Z.

An occupational therapist who had discussed this study with some of their clients echoed this point of view:

This project has come at the same time as a course we are having to teach older people IT. I had 16 people, and we went through your briefing pack together. When I mentioned your research about scams, once we started talking about it, other people started opening up about scams that have happened to them. I think that maybe an intervention that would probably be pretty good would be if we did have these kinds of courses out

there – IT courses for older people who would like to learn, and so that they can be with other people they can discuss it with together.

KT, whilst co-facilitating, recalled attending in a professional capacity a charity-organised coffee morning for older adults. He revealed that informal discussions around cybercrime uncovered a desire among attendees to ask more questions and share their experiences of cybercrime.

There were a lot of older adults there and there were questions about cybercrime and what they could do to safeguard themselves, and some of them did come up to me and said that they had been victims of cybercrime. Not very many had reported it. They didn't know what to do. So I think there is an element of value in finding places where older people are more likely to socialise and congregate, and targeting an intervention there.

5.4.1.2 Capitalising on the common desire to socialise and learn to impart cybercrime and reporting advice

Workshop participants also commented on how older adults value opportunities for social events and to learn about scams and cybersecurity, to impart their own knowledge on others, and that these discussions were destigmatising. An occupational therapist recalled one session attendee who wanted to learn and share her experiences:

I had a really old lady, I think she's late 80s, early 90s, but with very good advice that she started opening up about. She received a text message saying that her daughter dropped her mobile phone down the toilet, asking that she sends her some money. She actually got up out of her seat to come over to the flip chart that I had, to look at everything that I was writing down. Everyone seemed really interested in the topic of conversation as well, so maybe bring in IT courses and having those conversations might be less stigmatizing.

An older adult participant who volunteered for a UK Old Age charity spoke about the important social aspect of such sessions:

The reason I've come into contact with this [study] is because I volunteer at a session where they have dozens of people who go there just for a social event.

Another older adult raised how these sessions can also be held online, with the help of large charities and educational institutions, allowing people to attend irrespective of their geographical location.

Many people belong to U3A [University of the Third Age], for example, [it] has 400,000 members nationwide divided into over a thousand separate branches. It might be a very good idea to see if you can get some talks. Either a set talk that's given to local U3As, with trained speakers. And also the national organization does online talks – several a month – and that would be a very good way of reaching a number of people, although in all honesty it'll probably be about attendance of about 200 people at each zoom event. But it's [what is key] is trying to find the groupings of people I think. It's probably the most economical way of getting out information.

5.4.1.3 Providing educational resources with consistent messaging to aid session facilitators and for attendees to take home

Participants commonly remarked on the importance of providing course material such as guides, leaflets and posters for attendees and session organisers. Sourcing and funding these materials, as one older adult mentioned, could prove prohibitive for potential session organisers.

I think the important thing moving forward is to actually have some material available that can be put out to different organizations. The trouble is that most advertising actually costs you money, whether it's putting it on a bus or advertising in a newspaper. It all costs money. But having some kind of central message, imagine an A4 flyer perhaps, or even an A5 flyer initially, that can be distributed to lots of different places, or reproduced. It's also about encouraging dialogues as well; having discussions.

A second older adult recommended providing resources at these sessions as a means of taking home and storing useful information.

To have presentations there or just leaflets there – just some way of targeting the people who might be the victims and saying this is what's available to you [in terms of support and advice and reporting options]. I mean, even if it's not something that's immediately happening, it may be there for them in the future when they need it. It would have to be simple, it would just be, say, a saying if you think you have been a victim of this crime, these are the places you can go to. Leaflets, fridge magnets... whatever! Just a little trinket that has contact numbers on and things like that.

A security and justice advisory firm professional highlighted the importance of consistent messaging, pointing to previous anti-fraud campaigns that have each delivered different information.

One of the issues that we constantly come across is that fraud campaigns have not been successful due to the large amount of differing information that people are getting. The messaging is complicated, so any type of leaflets or fridge magnets will have to tie in with any national campaign that there is, so that the messaging is straightforward and consistent.

A psychiatrist remarked that such resources might be channelled, within health and social care organisations to local cyber 'champions' to facilitate and support their engagement with clients:

I think there is usually somebody that's a bit better at this stuff than others - and that's fairly resource neutral to have a team champion – and I suppose where this research could go would be to provide some resources for that champion, because you don't need very much, do you? You need the kind of basic advice that's sensible to give, and then

with ways of onward referring, perhaps with recommendations that if it's an online onward referral, they might want a sort of trusted person to help them do that.

5.4.2 Engaging previous victims of cybercrime to offer support and advice to older adults

An idea raised in the two workshops with professional stakeholders was to engage and involve former victims of cybercrime in activities; with the premise being that older adults would be more likely to talk about their experiences if they hear directly from another individual who has experienced cybercrime victimisation.

5.4.2.1 Setting up peer support helplines for victimised or concerned older adults

The security and justice advisory firm professional proposed a peer-led helpline that could be integrated into the services run by Action Fraud or a charity:

Something I was thinking about when you were going through your presentation – and I think it also links back to the importance of having people around you and to the previous point around making it easier to report through other means that aren't digital – is a helpline, but one that is run by other elderly people who previously may have also had experiences of victimisation. I think something similar has been done in Canada, but I'd have to double check that, but it would be a helpline that could be integrated into Action Fraud services or the third sector possibly, where elderly people are able to ring up to discuss their victimisation. They can then be referred onto other reporting mechanisms if necessary, or they can just have a chat about their experiences and any support that they might need. I think it's also valuable for those that run the helpline that have previously had experiences of victimisation to also help them overcome the feelings of blame, and understanding that this can happen to anyone really.

An Old Age charity digital specialist agreed with these comments:

I think that last point is good because that would reinforce the idea that it's...cybercrime is very common, and so individuals shouldn't feel ashamed of being scammed in some way because there are other people out there who they're talking to who have exactly the same experience.

5.4.2.2 Inviting previous victims to be guest speakers at cybersecurity sessions for older adults

Another way to engage former victims would be to invite them to speak about their experiences at cybersecurity events and sessions. A victim support charity manager who had organised such an event where a guest speaker was present indicated that it had been particularly successful.

We've gone to care homes... we've gone to town halls; anywhere that you can promote an event. And we have trialled that. So normally you do get people coming up afterwards, but when we've done a couple of sessions with victims, there was an even greater response because then you would get people in the audience who disclose that it had happened to them, but they hadn't reported it.

An occupational therapist remarked that having one person describe their experiences can spark group discussions:

[There is] a group that I that I run, and I run two sessions exploring new technologies and learning new skills. We're having these conversations about scams and things like that.... 'What are you worried about? – Well, I'm worried about cybercrime and things like that.' So I think by having these conversations, it's been quite nice. I mean, I said that "you know what? I was scammed on eBay" and then that's how we started off. I found out what people know and what people don't know. One person, he was scammed for £1400 and so then he knew about Action Fraud. He phoned them, Action Fraud got in touch with eBay, and he got his money back.

The victim support charity manager added that involving previous, older, victims may be more relatable than charity workers or the police:

So what we did trial as well was actually doing sessions with somebody who has been a victim. So now there's one thing isn't there from a professional like myself doing a full awareness session. If you've got someone next to me that they can really relate to – someone you know that looks like them - you know that has gone through a similar experience... that had a great initial buzz of people actually reporting. And once again, it's for people to know they don't necessarily have to report to the police. They can go to a charity like ourselves and still be supported. For whatever reason, people might not want to report to the police and that's fine. So they shouldn't think that, you know, is a barrier to them being supported generally.

5.4.3 Engaging younger demographics and other trusted individuals in educational and supporting roles

Another common suggestion was to promote support among families and wider communities. One occupational therapist advocated for a scheme that matches older adults in need of IT support with young people with considerable IT skills and knowledge:

We did have a charity, shut down now, [that was] bringing people together in the community. So a younger person would go around and teach an older person how to use IT. I thought that it's a shame that's not happening anymore, but that would have been quite helpful. They've done lots of different things, but that was one of the things that they used to do. Having younger people go around to teach older people to use IT just so that it could bring younger communities and older communities together more.

An Old Age psychiatrist suggested that a trusted friend or community member could assist an older person to report their crime online:

I do wonder whether a good piece of advice would be... because we have had a lot of people that have had a gutful of waiting on the phone being put on hold. I mean quite clearly the non-online reporting mechanisms cannot cope at the moment, and if somebody could find a trusted person to support them to use the online mechanisms. I just wonder whether that is [also] something that you could perhaps put in a video?

One older adult spoke about the potential for young people from minority ethnic communities to actively support their older family members and community members, who may not speak English as a first language, on all matters relating to scams and cybersecurity.

There are large communities where English isn't spoken at home really. You know, children and grandchildren would be the main sources of communicating with the older people in those families. I've seen it with my elderly in-laws. Anything in a way complicated would be dealt with through their children or grandchildren. When looking at how to get reporting done it's not just something about the older community. It's trying to tackle that next generation down, who are probably the people who are gonna often help the older community. Neighbours, the friends. The person at the church, or the synagogue, or the mosque, who might be the trusted person who they'll talk to.

5.4.4 Communicating messages that normalise and decatastrophise victimisation

All categories of participant discussed the need for public communications that normalise victimisation, and educate about cybercrime, in order that older victims of cybercrime feel less ashamed and more informed.

5.4.4.1 Emphasising victim faultlessness

Participants frequently remarked on how such communications must emphasise that the victim is not at fault, and that any practical advice given should be straightforward so as not to overwhelm the recipient or audience. One social worker spoke about a need to shift the victim blaming, overdramatic narrative to one that is calmer, more pragmatic and less judgemental.

So, [it is about] *almost normalising it... a shift from making it this really big, scary cybercrime, [where] terrible things are gonna happen, to 'this is something that's reality now a part of our everyday. This is how many people have been affected, but don't worry because there's this and this. And actually it's really common. It's not rare at all. You're not on your own. It doesn't mean you're going to lose all your money; you just have to do this to safeguard yourself. So like the shift from making it big and scary because, with the Internet, it's everywhere now. It's so common, isn't it!*

A victim support charity manager reiterated how important it is to communicate to older victims of cybercrime that they are indeed victims and should not feel responsible for the victimisation. They described the importance of publicising the Action Fraud replacement service, when it is eventually launched.

So firstly, on the 'you're not to blame' message, I think now we're getting a better understanding of the social grooming element, aren't we. So it's about coercion. So it's about, I think, always emphasising that message and [that] it's nothing to do with your intelligence. You know, you have been groomed, in effect, by the perpetrator. And in terms of where to go to for reporting. So Action Fraud as it stands is going through a rebirth. So when it is relaunched, as you know, the UK's reporting centre for fraud, how are people going to know about that? Obviously none of us know the answer to that at the moment, but how is that going to reach people? So I'll be watching that closely as well. It [Action Fraud] hasn't always been met with the most favourable response, shall we say, from its service users. So hopefully the feedback we'll get from people [regarding its replacement service] is that it's easier to speak to somebody [than with Action Fraud], that you are getting better two-way communication etcetera.

Multiple workshop participants emphasised the importance of destigmatisation; removing the shame and culpability entrenched in cybercrime victimisation by normalising it and showing people how to recover from it. As one older adult put it:

So there's something about education. It's okay to do this. Don't feel ashamed that you've been sucked in by somebody; a team of sophisticated people. They're very often scam teams, aren't they? It can happen to so many people so easily. I think shame is reduced by having more tools and knowing what to do.

One older adult suggested that communications should not necessarily be explicitly targeted at older adults, as this could heighten ageist societal and self-perceptions of susceptibility and gullibility.

I mean, I'm cynical. So you know I won't believe anything is true until I've done all the research to believe it is. But young people are being scammed too, so there's something about not the over sixties don't have to feel that they're in this group of being a bit dodgery and not quite being with it because it crosses all age ranges.

Another older adult remarked on the importance of reiterating that the crime could happen to anyone:

The other thing we've had this year is three or four different scams via telephone. I think they're just random. And I think that lots of older people feel that they've done something stupid that causes them personally to be targeted, whereas in practice it's random. You know, [begins to impersonate offender] 'we've got a mobile number, we're gonna try it and we'll see if we can get... you know... [some details]', and so I think people think they are personally being targeted, which immediately makes you shameful and vulnerable, rather than, you know, [recognising that] it's a fishing rod that's gone out trying to hook somebody. And so I think that telling you that that's what a lot of scams are, that they're just fishing – it's just a fishing expedition. I think that is something that would make people

feel more aware that things might be scams, but also help to reduce some of the shameful feelings.

5.4.4.2 Maximising message impact through TV and radio

Several participants suggested television and video as a medium for such communications, with many recalling television programmes or adverts that had made a lasting impression. One older adult spoke of the educational benefits of *Scam Interceptors* (Stapleton, 2023), a British factual television programme about online fraud:

I must say, I think that the program on BBC at the moment, the scam interceptors, to me, is very relevant. It opens your mind apart from anything else. I mean, I'm fortunate, I've never, ever had any approaches which have led to anything bad or anything. But really that sort of thing does open your mind. I really think it's a real eye opener.

Besides endorsements of longer programmes, participants made reference to how a short television advert, like that of the British Green Cross Code (Prowse, 2014) public road safety campaign that began in 1970, could be an effective way to impart crucial information about reporting options and also emphasise that they will be taken seriously:

I partly have visions of, you know, like a television ad. Really, the Green Cross Code man, when I was young, things that stick with you. But there are so many, I mean, people have such mixed views of reporting anything these days because of the reception they'll get. It's not worth the bother. Nobody cares. and I think it's raising the bar and saying, yes, there is care, and this is where you contact.

This sentiment was echoed by a second older adult, who remarked that many older generations still watch live television (as opposed to younger generations using streaming websites), and that this represented an opportunity to target older demographics:

I think that the Green Cross Code is quite, you know, simple and accessible too. I mean, older people tend to watch television and adverts on television still. So there's still mass

communication methods that older people are more receptive to than say younger people. So I think it's things like that, I think, would be useful to use.

One Old Age psychiatrist suggested the transmission of a short and simple video providing important security advice on screens at home and in public spaces:

I mean, it might be out there, but if there was a short two minute video that was endorsed by action fraud and so forth and gave the security information that was needed, then it could be shown in all of these different places. It could potentially be about building skills – you can get your clear message out.

This view was shared by an Old Age charity digital specialist:

So I'm thinking along lines of if you think you're a victim, this is the website. This is the e-mail address. This is the telephone number. So just a simple list of three or four different places to go.

A victim support charity manager added that any messaging needs to be clear and simple in order that the victim does not feel confusion or doubt:

[What is important is] making people aware of how they can report and who they should be reporting to, so there's no mixed messages or, you know, uncertainty around that.

Workshop participants acknowledged that any video or communications would need to be available in several different languages to reach all older victims of cybercrime in the UK, given the nation's considerable ethnic diversity. As one older adult said:

You would need to approach it with some multi-language communication. If you found there were particular communities being targeted, then you could tackle that. Or if each Borough Council had a reporting centre, they know the demographic of their people. They would know if there's a particularly Big Punjabi speaking population [for example].

Older adults may benefit from seeing or hearing from older victims of cybercrime on the television or the radio. As one older adult remarked, although their stories might make him feel wary, his overriding takeaway was encouragement:

I hear often on radio 4 the consumer programs, they quite frequently highlight scams and cybercrime issues, and we get stories of victims and how they've managed in most cases to seek redress. So I think there's quite a bit of information if you know where to look for there. They make me nervous initially, but then when I hear how people have resolved them, as is usually the case, I find that encouraging.

5.4.4.3 Making the most of NHS and care services to reach those in need of support

Participants also discussed the importance of using the full depth and breadth of care services to reach as many vulnerable older adults as possible – including those living in supported living accommodation and care homes – with key messaging around avoiding cybercrime and what to do if you do become a victim of cybercrime. As the victim support charity manager remarked:

It's always about how is that messaging going to cut through, isn't it? No doubt you would have come across this from your other working group with social care professionals, but it's about the people that are in old peoples' homes that may not be looking at, say, [victim support charity] Victim Support's social media for fraud awareness warnings. So it's about working with different services, isn't it. Care providers, etcetera.

One of the suggested ways to deliver important cybersecurity and reporting information was through posters and videos placed and screened in General Practitioner surgeries, of which there are thousands all over the UK in rural and urban areas. Older people are also more likely to visit their GP (Frese et al., 2016). As one older adult commented:

The other thing is, doctors' surgeries have huge notice boards targeting all age groups for things. So yeah, I just think the country needs to be swamped, young and old, with information about what to do [in the event of victimisation].

5.4.5 Training stakeholders on communicating empathetically and recognising victimisation signs

Another common theme that emerged during workshops was that the language and attitude of Fraud Justice Network employees can at times feel judgemental and blameful, with a lack of any real empathy or concern. The consensus was that training in this area might transform victims' reporting experiences and make them feel more comfortable engaging with the authorities or financial institutions regarding scams and cybercrime in future.

5.4.5.1 Using more empathetic and less victim blaming language when speaking with potential victims of cybercrime

Several older adults who had experienced cybercrime commented on how bank employees had spoken to them with a blameful and disinterested tone. For example, one older adult recalled an occasion when they had been made to feel fearful of being blamed:

In terms of these sorts of feelings of stupidity [experienced post victimisation], it comes back again to this training, or possibly it's not training, but attitude with the banks and the financial institutions. I was sending a large sum of money to a solicitor recently, and I called up [the bank], and the first thing they've done is ask 'where did you get the bank details from'. I said email, and they say 'oh well the emails could have been intercepted'. So they put this fear into you. There's this kind of tone, if you like. You get this sort of feeling of getting so fearful of making some sort of mistake which would lead you to being blamed for the fraud happening to you. And I understand that there has to be a balance, because obviously they're trying to protect you. I'm not quite sure what the answer is.

Another older adult echoed these views, explaining that negative, dismissive attitudes and language from the Fraud Justice Network might deter older adults from reporting victimisation again in future.

There is a sort of tertiary point here, I suppose there is something which crops up in my mind. I don't know if there's any stats on this. You know how many people report things that they think are a scam that turn out not to be. I think there's something here about how that's dealt with in terms of the people being made to feel stupid or embarrassed. It's the sort of 'cry wolf' thing, isn't it? If someone rings up, it's like, "Oh, no, don't be stupid". If the underlying attitude is, you know, a bit like when you get sent to Accident and Emergency by the doctor and the A and E people think "what are you doing here". That's the sense you get, you know. If that comes across on something which perhaps looks suspicious to you, but in fact not to be, could you potentially be dissuaded from raising [legitimate] issues?

One police fraud caseworker said that they were increasingly conscious of the type of language they use when speaking to their clients about their cybercrime experiences, recognising that it could come across as blameful or judgemental:

You need to be really careful in the use of language all the time. Like when I talk to people, they often say, oh, I feel really stupid that I fell for this. I'll always then want to explain to them that if it was any other crime, you wouldn't talk about having fallen for it, and people don't seem to view cybercrime as much of a crime as they would say Burglary or being assaulted or whatever. I think probably a lot of professionals are trying to change the way they frame things in the words that they use. But it's so ingrained that, you know, you fall for a scam. But it's kind of just like what people say without even thinking about it.

One older adult recalled a positive experience with a police officer, who was particularly empathetic, and his presence and language provided him and his wife reassurance:

My wife got very concerned about some scam that was going on – I don't remember, but she was so concerned. She reported it, and within an hour a young policeman knocked the door, and he was offering comfort and guidance. And we thought, 'wow', you know, 'I didn't expect that'. Every day I read the police neighbourhood reports, and a lot of them are related to scams. I will admit to finding the comfort of having this young six foot two young man, very interested, empathetic, but above all, it was giving my wife the confidence to know that there were genuine people out there, and these scammers probably just one in a million. Most of the people in this world, especially the British, are very caring, that's my experience. And they would do all they can to help keep the peace. I've got long COVID. My mind's going. I'm old. I can't remember what the scam was, but my wife at the time was quite concerned, and not only for herself, but for our daughter and other people. She did tick a box, in this report – 'do you want some kind of intervention or response?' And the thing is, we got it. To my surprise, my delightful surprise.

Another older adult told the workshop that he'd had a similar experience but with a physical crime, where the officer had been understanding and had made him feel heard, and that this alone was worth a lot regardless of the outcome of any investigation:

I had a similar very good experience like that with a burglary, actually, where the forensics guy suddenly turned up at my door because he'd heard the case on the [police] radio. If you feel vindicated and listened to, then that obviously to the average person is actually worth a lot. Or, you know, not only being listened to but the attitude when you're listened to – I think those two things couple together and are incredibly important in what we're talking about here.

5.4.5.2 Upskilling stakeholders to provide sound advice and to recognise and act on signs of victimisation

One health and social care professional mentioned that she will often discuss cybercrime with patients informally, but that she would benefit from some formal training on the subject:

Here, I do a 'lifestyle matters' programme. So we have these kinds of conversations and yeah, I must admit, we don't have the training on it really to talk about cybercrime. In fact, when it gets brought up, it's just a conversation that we end up having, a discussion about amongst ourselves. So yeah, I, we need to learn more.

KT remarked on the huge capacity of the NHS to reach a range of different individuals who may be being victimised:

One of the contributing factors [to victimisation] can be loneliness or loss of a spouse – going through a difficult period in their lives – and it's at that time when they're vulnerable that they need the support, but they don't seek it or don't know how to seek it. And the NHS has this huge, you know, network in place in order to do something about it, and to contribute to [tackling] it by identifying these individuals who are at risk or who are being victimised.

Regarding identifying individuals at risk, the health and social care professionals present advised that standard Care Act 2014 needs assessments do not currently reflect fraud or cybercrime risk.

5.5 Discussion

5.5.1 Summary of main findings

Participants co-created ideas for activities that could potentially respond to my previous study findings. They proposed cybersecurity group 'events' for older adults, held online or in person by a trusted person or organisation, with a degree of socialisation and interactivity. Older adult participants perceived benefits from such events, particularly if organisers have access to

materials to advertise sessions and enable attendees to “take home” key messages, for example on fridge magnets. Several participants proposed that previous victims of cybercrime could have an important role in these events, providing relatable lived experience to support others to share experiences and reducing stigma. A telephone or video ‘helpline’ with previous victims of cybercrime as call receivers was also proposed. Participants, assuming the existence of the digital divide, suggested that younger people could give IT help to older adults, or that older adults with limited English language ability could be supported by their children and grandchildren with translation of cybersecurity information and cybercrime reporting mechanisms. Participants remarked that victims would benefit from messaging that emphasises they are not to blame, that anyone can be victimised and that they’re not alone, recovery is achievable, and that there are people out there to provide support. In addition, such communications should not reinforce ageist societal perceptions around older people being vulnerable or gullible and should instead be framed as advice for all.

Many participants advocated for a media-based approach, citing a perception that older people are more likely to regularly watch ‘broadcast’ television with adverts than younger demographics. Participants across all workshops agreed that health and social care organisations and professionals are well placed to support with the delivery of these communications, both in terms of television screens in, for example, GP surgeries, and also on noticeboards in a variety of settings such as care homes. Participants also considered that stakeholder training around attitudes and language, victimisation indicators and reporting mechanisms would be beneficial, especially in the light of older group members experiences of unhelpful interactions when trying to report cybercrime.

The workshops revealed both alignment and divergence in the views and suggestions of older adults and professional stakeholders and health and social care professionals. There was broad agreement on the need to normalise victimisation and improve victim support, but with

differences in approach. Older adults preferred community-based discussions and relatable stories, while professionals leaned toward public information campaigns and staff training. It is important to note the role of professional stakeholders and health and social care professionals in representing and voicing the experiences of older adults they had worked with. However, their perspectives sometimes framed older adults as passive recipients of support, whereas older adults themselves emphasised autonomy and active participation in cybersecurity education.

5.5.2 Implications of findings

My findings of the value of the voice of lived experience are in line with a large body of evidence, including two recent studies. Choi et al.'s (2021) exploration of mutual disclosure among victims of sexual violence in Korea revealed that participants helped each other by assuming a dual role of help-seeker and support provider. Funston et al.'s (2023), exploration of the 'Insight Exchange' initiative in Australia found it went some way in shifting the domestic abuse and sexual violence victim blaming and shaming narrative. Based on the intervention proposals discussed above, one or more organisations from the Fraud Justice Network, might consider organising regular cybersecurity sessions for older people to educate on scams and reporting mechanisms and reduce the stigma associated with cybercrime victimisation. These could be hosted within, and with the support of, community spaces such as village halls and places of worship. Organisations with capacity to do so might wish to offer an online alternative. The government, or a coalition of financial institutions, may consider providing a centralised source of not only educational materials for attendees, but also written suggestions around session format, structure and content. The intervention I propose from the findings of this thesis, Online Porcupine (chapter 6), is strongly related to this particular point.

Participants drew on interventions that are already successfully supporting older adults with IT skills or in other areas. Helplines provide a safe space to talk about one's experiences, reduce distress and develop plans of action (Erbach et al., 2024) without being subjected to unsolicited

assessments, procedures and referrals by “insufficient, unhelpful and sometimes even damaging” professional services (Iversen & Westerlund, 2024). Age UK’s ‘Digital Buddies’ programme exists as a remote support service that matches anyone of any age with an older adult who is seeking help. Following training, reference and criminal record checks, digital buddies “develop a friendship over the telephone with an older person” and “support the older person to get online” and “work towards their chosen digital inclusion goals, e.g., using Zoom, search engines etc.” (Age UK, 2022). Investing in this and other existing programmes may be a cost-effective way to enhance cybercrime protective provision for older adults. It could be developed by engaging young people, perhaps who are in further or higher education and specialise in IT or other related subjects/fields, who are looking to build their experience. It might also be advertised to young people undertaking the Duke of Edinburgh’s Award scheme, of which volunteering is a significant part (DofE, 2022).

5.5.2.1 Participants considered how to target messages about cybersecurity to older people at risk.

One idea is to consider how to support grandchildren and other young people who might already be a bridge to English language resources for their grandparents. The 2021/22 census indicated that 16% of people in the UK – a total of around 10.7 million – had been born abroad (Cuibus, 2024). Of the 5.1 million people that reported they did not speak English as a main language, over a million reported not speaking English well or at all (ONS, 2022).

Participants considered older people major users of broadcast TV, a perception that is accurate according to UK’s communication services regulator (Ofcom, 2024). Television strategic communications campaigns, particularly in the context of health, have been found to be a powerful medium for disseminating public information and reducing stigma (Hu et al., 2017; Wallhed Finn et al., 2023).

My findings here are reflective of Shattered Assumptions theory; kind, attentive and non-judgemental reactions to victimisation by stakeholders can rebuild the victim's broken assumptions that the world is benevolent, meaningful and the self is worthy (Janoff-Bulman, 1999). Research indicates that police validation of victimisation experiences, and affirmation that the victim has been done wrong, is hugely important to the victim psychological recovery process (Elliott et al., 2014).

In addition to attitude and language, participants suggested that stakeholders, especially health and social care professionals, receive some cybercrime and cybersecurity training in order that they can engage clients in informed conversation about risks and reporting mechanisms, and also so that they can identify indicators of victimisation in clients, such as an unexplained lack of money or signs of distress or anxiety (SCIE, 2015).

5.5.3 Limitations

There are several limitations to this study. Firstly, workshops were held virtually, which offers considerable utility, efficiency and cost effectiveness (Rupert et al., 2017), and may be conducive to participants sharing sensitive information more candidly than they would do in-person (Woodyatt et al., 2016). It is plausible, however, that in-person discussions might have provided richer data, due to participants being able to build a rapport more easily and pick up on non-verbal cues. However, there is currently no empirical evidence that face-to-face focus groups or workshops give richer data than those held online. It is also probable that we were not able to reach older adults with limited access to technology, those who lacked confidence with technology, and perhaps also some of those who had experienced cybercrime and were nervous of engaging in any further online interactions. These individuals might actually have been at greatest risk of cybercrime.

Secondly, my health and social care participants, professional stakeholder participants and older adult participants did not have any direct communication with each other, because each

participant group had its own workshop. I opted for this design because I felt the discrepancies in experiences and subject-specific expertise would act as barriers to clear and flowing conversation in which all participants felt comfortable engaging. However, this meant that each category of participant was not able to interact, and therefore react and respond to each other's comments and suggestions. In other words, potential intervention end users – i.e. older adults – could not directly voice their opinions on the ideas generated by professional stakeholders and health and social care professionals to those individuals. Conscious of this limitation, I decided to hold my professional workshops first and my older adult workshops last, and carry over summaries of the most pertinent topics of conversation and intervention ideas from each workshop to the next. These summaries formed part of my workshop introductions.

Another limitation is that I was unable to recruit stakeholders from financial institutions. This is a notable omission in terms of expertise, for example knowledge of reporting mechanisms and existing interventions. Critically, Action Fraud was not present in this nor the previous study, despite being invited to participate. Action Fraud is set to be replaced by an alternative service later in 2025 (Martin, 2024).

Another limitation is that, as per the MRC Developing and evaluating complex interventions framework (figure 5.1), this study represents only one part of the intervention development process. Though multiple ideas were generated, the feasibility of those ideas was not considered in great depth. The implementation and evaluation of an intervention would follow a feasibility study.

Finally, although participants were invited to help structure our conversation by contributing to the theory of change via the online whiteboard, participants – and in particular the older adults – were not invited to plan or facilitate any of the workshops or participate in the analysis of transcripts. Co-design refers to the “creative cooperation during design processes (...) [where] diverse experts come together, such as researchers, designers or developers, and (potential)

customers and users—who are also experts (...) to cooperate creatively”. It represents an organisation of the creative process that bridges the gap between key stakeholders in order to combine capabilities and provide a better fit between the provider and the end-user (Steen et al., 2011). It has been widely used in the development of interventions to help vulnerable people overcome various challenges, including people living with dementia to promote social inclusion (Innes et al., 2022; Jones & Miesen, 2004) and cyber safety training resources for people with brain injuries (Carminati et al., 2023). Incorporating co-design principles more is something I will be looking to address in any future development of the ideas generated during this study.

5.5.4 Conclusions

Barriers to reporting cybercrime faced by older adults include shame and embarrassment, difficulties experienced in the reporting process, and a lack of awareness of reporting options and sources of support. When asked how to address these barriers, older adults, health and social care professionals and other relevant stakeholders proposed destigmatising communication campaigns including through television and radio, the engagement of younger demographics and previous victims in supporting roles, greater employee training to address the victim-blaming narrative and increase guardianship, and finally, interactive cybersecurity sessions for older adults that raise awareness and encourage sharing between peers and facilitators.

In chapter 6 I will present my intervention idea, Online Porcupine, which incorporates several of the aforementioned activities and activity components. Finally, in Chapter 7, I will discuss all the main findings from my three research projects, along with the thesis’ strengths, limitations and implications.

Chapter 6: Developing an intervention to protect older adults from cybercrime: Online Porcupine

In this chapter I describe how I used the consultations I described in Chapter 5 to develop a prototype for an intervention, which I have named online porcupine (www.onlineporcupine.com). Online Porcupine would be a social enterprise or charity that provides resources and guidance to help local community organisations facilitate their own friendly and accessible interactive cybersecurity sessions for older adults. The aim of Online Porcupine sessions is, firstly, to educate about different cybercrime types and the different sources of support and reporting avenues available to victims or potential victims, and secondly, to create a supportive environment that encourages discussion, sharing and mutual support, thus breaking down the stigma and ageism that exists around cybercrime victimisation and use of technology in old age. I describe how my plans for online porcupine map on to my findings, and how I plan to develop it as part of my post-doctoral work.

6.1 Why the Name?

The porcupine is a hardy rodent with a very clever defence mechanism. Though they may not be the fastest animal on the planet, their coat of spines or quills protects against predation, enabling them to remain calm under threat and go about their business with confidence.

6.2 How does it aim to protect older adults from cybercrime?

Online Porcupine aims to protect older adults from cybercrime by empowering them to recognise and report cybercrime so that an appropriate third party can intervene, minimise the harmful financial and emotional consequences, and reduce the chances of victimisation and/or repeat victimisation. It also aims to lessen the impact of secondary victimisation and shattered assumptions by equipping attendees with a realistic understanding of what cybercrime is, who

commits it, who can become a victim (anyone), how to report it, and what to expect from the financial and criminal justice systems.

6.3 How does it work?

Each month, Online Porcupine would put together the structure and content of a session, ready to be picked up and facilitated by local community organisations such as supported living accommodations, charities, places of worship and village halls. An Online Porcupine session could be incorporated into a pre-existing offering such as a monthly get-together, or it could become an entirely new one-off or regular event.

Facilitators of Online Porcupine sessions will be able to download and print all the materials relating to that month's session from the website, including readings, videos, audio recordings, hand-outs, posters and pictures, all designed for consumption by non-experts and informed by key literature surrounding the development of educational materials for older adults, e.g. Ahmad et al. (2022), Cjaza et al. (1994), Farage et al. (2012).

Online Porcupine sessions can be held virtually via video conference (e.g. Microsoft Teams or Zoom), or in person in private or public spaces. The facilitator will also be given a step-by-step guide to hosting the session, along with thought-provoking prompts and conversational points. Each month will focus on a different topic, whether that's a crime type or a security measure. The sessions will aim to be as fun and light-hearted in nature as possible, though attendees will be given the opportunity to speak to the facilitator privately in case they have any concerns or experiences they wish to share without drawing attention to themselves. Online Porcupine facilitators will be equipped with a full list of support contacts and will be given guidance on how to respond to reports of victimisation, including cases whereby alerting the authorities is appropriate.

It is hoped that organisations such as the police, victim support charities, Action Fraud, Trading Standards, and banks will endorse and partner with Online Porcupine. Facilitators will be able to contact said partnered organisations and request their attendance at Online Porcupine sessions as guest speakers, even if it is via video link.

6.4 How does Online Porcupine draw on my consultation findings and previous research?

In this section, I will describe how Online Porcupine delivers against a number of the findings and recommendations that have emerged through my three research projects, as well as from the existing body of evidence. Table 6.1 demonstrates how the design of online porcupine maps to consultation findings.

Table 6.1: Demonstration of how Online Porcupine design maps to consultation findings

Activity	Activity Component	Proposed Online Porcupine design
Holding interactive cybersecurity sessions that bring older adults together	Creating an environment that allows older adults to feel comfortable about opening up	<ul style="list-style-type: none"> • Educates attendees on cyber risks and cybersecurity in order to improve detection and prevention skills • Guides attendees through correct ways of reacting to and reporting cybercrime • Provides a safe, welcoming and judgement-free space where negative stereotypes are challenged, and attendees feel comfortable opening up and sharing their experiences with friends and trusted facilitators • Brings people together to engage and interact with new and old friends, to chat about life and to provide mutual support. • Virtual sessions have the capacity to reach socially isolated individuals
	Capitalising on the common desire to socialise and learn to impart cybercrime and reporting advice	
	Providing educational resources with universal messaging to aid session facilitators and for attendees to take home	
Engaging previous victims of	Setting up peer support helplines for victimised or concerned older adults	

cybercrime to offer support and advice in different contexts	Inviting previous victims to be guest speakers at cybersecurity sessions for older adults	<ul style="list-style-type: none"> • Offers a space for redemptive storytelling – the sharing of stories of trauma and self-identification as a survivor to a public audience
Engaging younger demographics and other trusted individuals in educational and supporting roles	Organising IT help schemes where younger people are matched with older adults in need of IT support	<ul style="list-style-type: none"> • Made available in those languages whose speakers have the lowest attainment in English • Publicised in areas with large ethnic minority populations • Offers volunteering opportunities to individuals doing schemes such as the Duke of Edinburgh's Award or Scouting Awards
	Translating and interpreting of cybersecurity advice, cybercrime reporting processes and potentially malicious communications by younger people for older adults whose first language is not English	
Communicating messages that normalise and decatastrophise victimisation	Emphasising victim faultlessness	<ul style="list-style-type: none"> • Provides straightforward and easy-to-digest educational advice • Provides physical resources for attendees which contain consistent, practical advice and friendly cybersecurity reminders • Incorporates a range of audio and visual content • Talks about cybercrime sensibly and pragmatically, breaking down its mystery and grandeur, and empowering attendees to use the internet with confidence and to report threats calmly
	Maximising message impact through television and radio	
	Making the most of NHS and care services to reach those in need of support	
Training stakeholders on communicating empathetically and recognising victimisation signs	Using more empathetic and less victim blaming language when speaking with potential victims of cybercrime	<ul style="list-style-type: none"> • Engages the FJN and health and social care professionals – whether that is in terms of session facilitation, providing resources, or inviting guest speakers • Builds the relationship between those professionals and older adults, creating an opportunity to learn from one another so that future dealings are more productive and appropriate and secondary victimisation is minimised
	Upskilling stakeholders to provide sound advice and to recognise and act on signs of victimisation	

6.4.1 'Holding interactive cybersecurity sessions that bring older adults together'

The data from my quantitative study suggested that older adults were more likely than younger demographics to suffer repeat cybercrime victimisation and associated financial loss. My results were also suggestive of underreporting by older adults. Furthermore, my second, interview study

on the barriers to reporting revealed a mixed understanding of different cybercrime types and reporting mechanisms. Online Porcupine will educate older adults on cyber risks and cybersecurity in order to improve their own detection and prevention skills. The sessions will also guide attendees through the correct ways of reporting cybercrime, including with financial institutions, so that victims receive the support they need to recover and are less likely to be victimised a second or third time. As per Farrell & Pease's (2017) tenets of repeat victimisation, victims of crime experience a higher risk of future victimisation immediately after initial victimisation. That is why Online Porcupine will teach attendees exactly what to do as soon as possible after experiencing a cybercrime incident.

In my second study, older adults frequently remarked on feeling guilt or shame following victimisation, which is intrinsically linked with ageist victim-blaming attitudes and, as per Rosales et al.'s (2023) conceptual model of digital ageism, societal and corporate perceptions of older people being gullible and less capable using technology. In my third study, stakeholders referred to the importance of creating spaces where people can chat about the subject with trusted individuals and peers. Online Porcupine will provide a safe, welcoming and judgement-free space where negative stereotypes are challenged, and attendees feel comfortable opening up and sharing their experiences with friends and trusted facilitators. This element of Online Porcupine aligns with the findings of Button et al. (2024), whose research into delivering fraud prevention advice to older adults revealed that the most effective means of disseminating advice is via interaction with friends and trusted individuals, and that charities and social service organisations can act as trusted individuals with limited social networks.

Online Porcupine would also help tackle loneliness and social isolation. In-person sessions bring together people to engage and interact with new and old friends, to chat about life and to provide mutual support. Virtual Online Porcupine sessions have the capacity to reach very socially isolated individuals in society; providing a platform for those who cannot leave home to

participate in any sort of social gathering. Furthermore, loneliness and social isolation have been identified as risk factors for cybercrime victimisation. According to Burton et al. (2022), social isolation and limited social networks increase vulnerability to online fraud and scams, as individuals may be more inclined to engage with fraudulent actors who appear to offer companionship or support.

6.4.2 ‘Engaging previous victims of cybercrime to offer support and advice in different contexts’

Besides fostering connections, strengthening community ties, and providing a safe space where individuals can discuss cybersecurity concerns without fear or shame, Online Porcupine would offer a space for redemptive storying, both by regular attendees and also guest speakers. Redemptive storying is the sharing of stories of trauma and self-identification as a survivor to a public audience (Delker et al., 2020). Crime victimisation can entail the loss of agency, control and choice. If attendees are able to speak out about their experiences, this represents a form of resistance against societal stigma that can be empowering and self-healing for themselves and for others; such attendees would also assume an ‘advocacy’ role, acting on behalf of other victims present at Online Porcupine sessions.

6.4.3 ‘Engaging younger demographics and other trusted individuals in educational and supporting roles’

In my second and third studies, participants raised the idea of IT help schemes where younger people are matched with older adults in need of IT support. Online Porcupine would seek to facilitate this type of engagement by partnering with schools, Scouting and Guiding organisations and potentially other youth groups to create volunteering opportunities at Online Porcupine sessions. Online Porcupine might seek to become an ‘Approved Activity Provider’ of the Duke of Edinburgh’s Award, for example – a youth awards programme which is often facilitated by Schools and has a volunteering component (DofE, 2024).

In my first study, I found that people of Black and mixed or multiple ethnicities were significantly more likely to experience victimisation and repeat victimisation than White people. This aligns with the findings of Salisbury and Upson (2004), whose crime survey analysis found that people of Black and minority ethnicity are more likely than White people to fall victim to crime in general. In both my second and third studies, reference was made to sections of the UK population who do not speak English as a first language, and the challenges they might face when navigating the internet securely and reporting cybercrime. Online Porcupine content will, in time, be made available in those languages whose speakers have the lowest attainment in English (i.e. for whom English is not a realistic alternative). Further research is necessary to establish which languages would be prioritised. Special efforts will be made to publicise Online Porcupine in areas with large ethnic minority populations. Again, further research would be required to inform this.

6.4.4 ‘Communicating messages that normalise and decatastrophise victimisation’

A core part of Online Porcupine’s offering will be the provision of physical resources for attendees. In my third study, older adults commented on their desire for more physical aids such as posters, fridge magnets and leaflets to help them remember the basics of what can be a complicated subject. Participants also remarked on how cybersecurity messaging can be convoluted, and that there are multiple different messages coming from multiple different organisations which are sometimes contradictory. These physical resources – which will contain consistent practical advice and friendly cybersecurity reminders – will be downloadable (for printing) or orderable from the Online Porcupine website. They will exist alongside all of the other resources provided to session facilitators. Crucially, they will be the same nationwide, and the messaging will be simple and consistent. All materials will be designed in accordance with the findings of Goodman & Lambert (2023), whose scoping review of the preferences of older adults for health-related education materials highlighted a number of favoured characteristics which I determine to be generalisable to the context of crime prevention, including: short, headed

sections; 1.5 or double line spacing; relatively large sans serif fonts; and content that exhibits diversity but with representation of, and relevance for, older populations.

Several participants across studies 2 and 3 commented on how they have particularly engaged with, or remembered, television and radio shows about cybercrime and cybersecurity, citing their effectiveness in sharing important information in a memorable and entertaining way. Online Porcupine will incorporate a range of audio and visual content into its offering. This could be anything from radio conversations to original role plays to television episode snippets. They will be used as a prompt for discussion among attendees. Button et al.'s (2024) research revealed that a multi-media approach increases the chances of engagement among older adults due to variations in preferred watching, reading or listening habits. The video and radio content shown at Online Porcupine sessions will also be informed by Pryor & McLaughlin (2018), who produced a series of literature-based recommendations on educational multimedia for older adults. This includes conveying subject-specific content only, and presenting the same or similar instruction consistently across multiple modalities in order that the recipient is not overwhelmed with superfluous or contradictory information. All educational advice provided will be straightforward and easy to digest, as recommended during my stakeholder workshops, and will hopefully rebuild a level of confidence among those attendees who have been unsuccessful in reporting cybercrime previously and as a result hold feelings of 'learned helplessness' (Maier & Seligman 1976).

When discussing barriers to reporting, a number of older adults cited a fear of repercussion as a reason for not disclosing their victimisation to the bank or authorities. Further discussion with these and other individuals indicates that their overly-fearful perceptions of cybercrime and cybercriminals were influenced by television programmes such as 'Scam Interceptors', which, although entertaining, transmit deliberately unrepresentative content about particularly extreme cases, using music and visual effects to heighten the drama. Ceccato (2016) found that concerns

around crime and insecurity among older adults are related to the social construct of ‘danger’, which is fed by mass media and social media attention, which in turn provoke social interaction and generate public anxiety. Online Porcupine will talk about cybercrime sensibly and pragmatically, breaking down its mystery and grandeur, empowering attendees to use the internet with confidence and to report threats calmly.

6.4.5 Training stakeholders on communicating empathetically and recognising victimisation signs

In study 2, I found shame and perceptions of reporting as being unhelpful to emotional recovery and as barriers to reporting cybercrime among older adults. In study 3, workshop attendees suggested that these barriers could be mitigated if stakeholders, such as FJN employees, used more empathetic and less victim-blaming language when dealing with victims or potential victims. It was also suggested that these stakeholders, including health and social care professionals, need greater training around recognising the signs of victimisation. By engaging the FJN and health and social care with Online Porcupine – whether that is in terms of session facilitation, providing resources, or inviting guest speakers – we will build the relationship between those professionals and older adults, creating an opportunity to learn from one another, so that future dealings are more productive and appropriate, and any secondary victimisation is minimised.

6.5 Other considerations

Further research will be needed to determine the logistical aspects of running Online Porcupine sessions such as time and day of sessions and entry criteria, and the extent to which such decisions will be made centrally or by session facilitators.

As a former police officer, I am aware that there may be a small number of predatory individuals who might look to attend, befriend and take advantage of other (vulnerable)

attendees, a phenomenon known as Mate Crime (Doherty, 2015). Though normally applied to the befriending of people with intellectual disabilities (e.g. Tharshini, 2024), it also applies to older adults – a context more commonly discussed under the umbrella of financial exploitation or abuse (e.g. N. G. Choi et al., 1999; Soliman & Beaman, 2014). Facilitators would be given guidance around recognising instances of Mate Crime and the options at their disposal to address it, similar to that offered by the Association for Real Change (2013). This includes: spotting victimisation indicators such as weight loss, changes in routine, or the appearance of a new ‘friend’ who undermines the individual; building relationships with neighbourhood police officers; and improving links with safeguarding agencies.

6.6 Scaling up Online Porcupine

Finally, I would like to conduct further development of the Online Porcupine prototype, beginning with more research. Specifically, I would look to apply for funding to conduct co-design workshops – actively involving older adults in leadership roles – as well as inviting experts in digital content and adult education and training. Once my prototype is refined, I will begin to build the content for a number of Online Porcupine sessions, as well as a ‘how-to’ guide for session facilitators. I may then approach some of the charities with whom I have built relationships - and who already run different events for older people – to gauge the possibility of actually conducting some pilot studies. Depending on resources, these could possibly be in the form of a feasibility study or even a randomised control trial (RCT) with different populations to determine not only Online Porcupine’s effectiveness as an intervention, but also best methods of implementation (Bernet et al., 2013). Through participant surveys, I might measure outcomes such as knowledge of cybercrime reporting options, knowledge of cybercrime types, enjoyment of session and ease of session. I would then continue to refine the Online Porcupine model and develop more session content, as well as considering its long-term feasibility and sustainability as a social enterprise, looking at factors such as funding, costs, investment, revenue streams, sponsorship, licensing,

staffing and website upkeep. There may be scope for affiliation or partnership with a university or financial institution. For me or whoever takes charge, it would represent a full time endeavour.

6.7 Example Online Porcupine Session Structure

The following is a demonstration of an overview, for facilitators, of an Online Porcupine session.

Online Porcupine

www.onlineporcupine.com



Pack 1: *Scam type* / *Organisational focus*

1. Introductory Video about *scam type*
link
10 minutes
2. Small group/pairs discussion
How would you recognise this scam?
What are the red flags?
(Facilitator then requests volunteers)
5 minutes
3. Radio excerpt
Previous victim talking about *scam type*
victimisation
5 minutes
4. Whole group discussion
Prompts:
 - *Question 1*
 - *Question 2*
 - *Question 3*10 minutes
5. Guest speaker
Plus Q&A
10 minutes
6. Refreshments and chatting
20 minutes

Physical resources for order or print at home available at:

www.onlineporcupine.com/pack1/resources
Pack 1 resources include:

- Accompanying PowerPoint presentation
- Leaflet on *scam type*
- Fridge magnet on *scam type*

This pack and accompanying resources are available in 5 different languages. Visit www.onlineporcupine.com/language for more information.

If you would like to speak to somebody from Online Porcupine about this pack, please send a message and your number to *email address* and we will get back to you ASAP.

We have compiled a list of organisations that have indicated they could be willing to provide a guest speaker here:
www.onlineporcupine.com/guests

Chapter 7: Discussion

7.1 Summary of findings

This thesis investigates how older adults experience, respond to, and report cybercrime, with the aim of developing strategies to increase protective behaviours, primarily reporting, and reduce the harm and stigma associated with victimisation.

Older adults have often been assumed to be at higher risk of cyber victimisation due to social isolation, declining health, and lower digital literacy. However, the findings of study 1 suggest older adults are typically less likely to report minor cyber incidents and, paradoxically, more likely to experience repeat victimisation with a significant financial impact. This discrepancy suggests that many offences go unreported until they become severe enough to trigger meaningful help-seeking or involvement of third parties such as banks or family members. Study 1 also revealed that cybercrime victimisation was associated with characteristics such as Black, mixed and multiple ethnicity, male sex, living in less deprived areas and poor general, mental, physical and cognitive health.

In order to explore the potential reasons behind the pattern of putative under-reporting in study 1, in study 2 I conducted individual interviews with older adults, their family members and a range of professional stakeholders. The interviews revealed that under-reporting stems from a combination of personal, structural, and sociocultural factors. Shame and fear of being seen as gullible or technologically limited, captured under the concept of interpersonal digital ageism (Rosales et al., 2023), were commonly mentioned among older victims. Anxieties about protracted or futile reporting processes discouraged many from contacting the police or financial institutions. Previous negative interactions with the FJN (suggestive of corporate digital ageism (Rosales et al., 2023)) reinforced feelings of helplessness.

In study 3, I shared these insights with workshops of health and social care professionals and other professional stakeholders (i.e. potential intervention implementers) as well as older adults (i.e. potential end users or intervention beneficiaries), in order to generate evidence-informed intervention ideas. Participants suggested group sessions – online or in-person – run by trusted community organisations, which could include take-home resources (e.g., fridge magnets) and first-hand accounts from previous cybercrime victims to reduce stigma. In chapter 6 I described how my proposed intervention Online Porcupine stems from this data. A phone or video helpline, staffed by older volunteers who had previously been victimised, was proposed, alongside younger relatives helping with digital or language barriers. Participants emphasised messaging that avoids ageist stereotypes and reassures people that anyone can be a victim without blame. They recommended the use of traditional media like TV and radio, as well as displays in health and social care settings, for sharing advice. Professionals and older adults broadly agreed on the need to ‘normalise’ victimisation and strengthen support services. In Figure 7.1, I illustrate my research pathway: from analysing CSEW data in order to explore the relationship between cybercrime victimisation, repeat victimisation, financial loss, age and other sociodemographic characteristics in the UK; to holding individual interviews with cybercrime victims and other stakeholders in order to understand possible barriers to reporting; to hosting stakeholder workshops to generate intervention ideas; and finally to developing an intervention prototype.

Figure 7.1: Finding, consultation, prototype illustration

Findings: CSEW analysis & one-to-one victim & stakeholder interviews

Study 1: Older adults more likely to suffer repeat victimisation & financial loss, but less likely to report single incidents or incidents without financial loss, which could be suggestive of underreporting. Cybercrime victimisation associated with poor health, being Black or of mixed/multiple ethnicities, & being male

Study 2: Shame & fear of repercussion influenced by ageism; unhelpful reporting procedures; & limited knowledge of scams & sources of support represented barriers to reporting

Sharing experiences with supportive and trusted peers & professionals can give confidence & be informative

Consultation: Workshops with older adults, professional stakeholders and health and social care professionals

Study 3: 5 key activities to increase cybercrime reporting among older adults, based on findings and fresh insight:

(1) Holding interactive cybersecurity sessions that bring older adults together; (2) Engaging previous victims of cybercrime to offer support and advice in different contexts; (3) Engaging younger demographics in educational and supporting roles; (4) Communicating messages that normalise and decatastrophise victimisation; (5) Training stakeholders on communicating empathetically

Prototype: Online Porcupine

What is it? A social enterprise or charity that provides resources & guidance to help local community organisations facilitate their own friendly & accessible interactive cybersecurity sessions for older adults.

What is the aim? (A) To educate about different cybercrime types, sources of support & reporting avenues; (B), to create a supportive & upbeat environment that encourages discussion, sharing and mutual support, thus breaking down stigma & ageism that exists around cybercrime victimisation & use of technology in old age.

7.2 Interpretation of findings

A central finding of this thesis is that older adults, despite often spending less time online, may face heightened likelihoods of severe or repeat cyber victimisation. The Routine Activities Approach (Cohen & Felson, 1979) proposes that crime occurs when a motivated offender converges with a suitable target in the absence of capable guardianship. One would ordinarily expect less ‘exposure’ (i.e. time online) to decrease victimisation risk; however, our data suggest that although older adults may have fewer ‘routine’ opportunities to encounter offenders, their level of ‘guardianship’ may be low (e.g., less social or digital support, or less capability to recognise scams), and older adults may also be perceived as more ‘suitable targets’ (e.g., with savings and more trusting attitudes).

The strong influence of societal stigma, shame and embarrassment on reporting resonates with Shattered Assumptions theory (Janoff-Bulman, 1999). Participants’ accounts revealed a crisis of self-trust and self-worth, reflecting how victimisation can topple one’s belief in a predictable and fair environment. Online Porcupine – an amalgamation of the intervention ideas generated in my third study, all centred around friendly and non-judgemental cybersecurity peer-support sessions for older adults – might be conducive to the reconstruction of shattered assumptions for any victims in attendance, thus assisting their recovery. Moreover, for those who have not been victimised, Online Porcupine sessions should preemptively ‘harden’ those assumptions by delivering realistic and helpful information and advice so that – in the unfortunate event of victimisation – the victim is not taken by surprise and is equipped to respond in the best way possible.

By internalising ageist and digitally ageist stereotypes (Rosales et al., 2023) such as older adults being technologically limited, victims felt doubly undermined: not only were they defrauded, but they feared censure for lacking the know-how to avoid it. This finding supports previous work

(Button et al., 2024; Cross, 2013) showing that shame hampers help-seeking, and emphasises how ageism amplifies it. If 'secondary victimisation' is when a victim of a crime suffers further negative consequences and harm from their contact with societal institutions such as law enforcement and the criminal justice system (Pemberton & Mulder, 2023), then a central theoretical contribution of this thesis is that the oppressive shame stemming from broader societal stigma around cybercrime victimisation and the supposed gullibility of older adults represents a form of tertiary victimisation.

A further strand concerns social support, which emerged as important in restoring emotional wellbeing and facilitating disclosures. Numerous participants cited family, peers, or trusted community figures as sources of reassurance and practical guidance. This reinforces evidence that robust support networks protect older people from adverse outcomes (Cooper et al., 2021). My research extends that insight by applying it specifically to cybercrime contexts. Here, the proposed interactive cybersecurity sessions aim to normalise talk about scams and indeed victimisation, echoing the peer-led approaches proven effective in other domains (e.g., chronic illness management), yet less studied in cybercrime victimisation (Karagiannopoulos et al., 2021).

My initial intervention prototype Online Porcupine aligns with Situational Crime Prevention techniques (Clarke, 2017) by altering immediate conditions around older adults' online activities. Raising awareness of different cybercrime types, how to protect yourself and your assets, and FJN reporting channels are manifestations of 'increase the effort', 'increase the risks' and 'reduce the rewards'. It also speaks to Routine Activities. By embedding supportive, empathetic communication and normalising victimhood experiences, the intervention aims to boost guardianship through community networks.

7.3 Strengths and Weaknesses

7.3.1 Strengths

7.3.1.1 *Stakeholder participation*

In studies 2 and 3, I sought to elicit the views of older adults, alongside a range of different professional stakeholders. In study 2, I spoke to individuals one-to-one in order gain real-life insight around their reporting experiences and/or decision making processes. In study 3, I brought together older adults and other stakeholders to idea storm potential interventions that would increase cybercrime reporting among that demographic. Through this PPI consultation approach, I sought to ensure that my recommendations are relevant to the actual circumstances and preferences of people with relevant lived experiences (Biggane et al., 2019).

I did not however coproduce my research or ‘co-design’ my prototype intervention. Originally, I had intentions of co-design – I had initially named the study ‘Co-designing interventions to tackle digital ageism around cybercrime victimisation’. However, on reflection, the study does not amount to co-design because the ‘locus’ of control and agency to make important, overarching, decisions sat with me, rather than being distributed equally among participants, as per Peacock's (2022) definition. Instead, I propose that my research can be defined as adopting a ‘participatory’ design or research approach. Morrow (2022) defines this as “the act of utilizing research participants as experience experts” in order to “uncover their own unmet needs and unrealized desires which can then be used as design drivers”. The researcher retains an enabler or facilitator position. By actively encouraging participants to shape the structure of workshop conversation through amendment of our theory of change on Jamboard, we encouraged a level of participatory engagement that goes beyond a simple consultation. In any future development of the Online Porcupine prototype, I might indeed look to engage participants as co-designers.

7.3.1.2 *Incorporation of anti-digital ageism research principles*

In my research design, I have endeavoured to avoid reproducing age-related stereotypes. Garavaglia et al. (2023) reflected on their own research on ageing and digital technologies and found that – despite explicitly rejecting stereotypical representations of older digital technology users as intrinsically deficient – they too excluded the very oldest individuals due to their presumed technological limitations. Conscious of this stereotype, I deliberately did not implement an upper age limit on participation for my studies, though there were no volunteers aged over 79. Garavaglia et al. (2023) also reflected on the importance of a flexible research design that is adaptable for heterogeneity in older adult’s digital technology ability. In my second study, I offered participants a choice of virtual or in-person interviews to account for differing preferences or needs. In my third study, I remained open to special requests for in-person workshops which I would have facilitated had there been demand.

7.3.2 Weaknesses

7.3.2.1 *COVID-19*

This thesis spans the onset and aftermath of the COVID-19 pandemic. While some research (such as the quantitative survey analysis) was based on pre-pandemic datasets, other components (particularly interviews and workshops) took place amid or after social distancing measures had potentially shaped new digital habits, such as adoption of digital health services (Haimi & Sergienko, 2024). Because the pandemic triggered a marked shift in older adults’ reliance on digital technologies – both for social interaction and essential services (Sixsmith et al., 2022) – part of the thesis reflects pre-pandemic conditions that may have subsequently evolved. Although this tension is not unusual given the unprecedented global disruption, the interpretation of any comparisons between older and post-COVID contexts should remain tentative.

7.3.2.2 Overarching treatment of cybercrime

Although this thesis addresses a range of cybercrimes encountered by older adults, from phishing and investment scams to romance and consumer fraud, some of the analyses – e.g. my CSEW study – treated ‘cybercrime’ as a broad category. This approach risked overlooking nuances that might distinguish, for example, social engineering scams from hacking or malware. Tcherni et al. (2016) stress that some types of online crimes, such as credit card fraud involving the theft of physical paper documents, have significant offline components with differing means of victim exploitation. Future research would benefit from more granular distinctions among offence types, as they may follow different victim-offender dynamics and require tailored prevention or reporting channels.

7.3.2.3 Self-reporting

The thesis acknowledges that embarrassment, shame, or fear of judgment can hamper victims’ willingness to disclose incidents fully, whether in large-scale surveys or personal interviews. Although every effort was made to create a safe environment in my qualitative studies, the possibility remains that some participants underreported or framed their victimisation narratives in ways that minimised distressing details or assigned blame away from themselves, thus affecting the accuracy or completeness of victim accounts (Reep-van den Bergh & Junger, 2018). Similarly, self-reported data in the CSEW may have been influenced by unawareness of victimisation due to the hidden nature of certain cyber offences such as malware, or alternatively because the victim has been reimbursed and therefore does not perceive themselves to be a victim (McGuire & Dowling, 2013).

7.3.2.4 Absence of offender perspective

Additionally, the thesis did not include offender perspectives. The few studies that incorporate insights from former or active offenders (e.g. Aransiola & Asindemake, 2011; Hutchings & Holt, 2018) suggest that they are dynamic in their decision making according to the context and target,

including references to perceived ‘easier’ characteristics or specific situational triggers. Incorporating such perspectives in the future could add critical context to the victim experiences documented here and potentially sharpen the preventive measures proposed.

7.3.2.5 Lack of participant diversity

Lastly, although the quantitative findings highlighted that certain groups are at elevated risk of cybercrime (for example, those from Black or mixed ethnicities in England and Wales), the subsequent qualitative projects did not fully reflect that diversity. Underrepresentation in research represents a failure to capture the complex, nuanced and unique lived experiences of different groups within society. This is particularly problematic if the purpose of the research is to inform policy, products or services that benefit an entire population or a cross-cutting age group; only the represented benefit and so existing inequalities are actually reinforced (Bibbins-Domingo & Helman, 2022). Recruitment primarily engaged those willing to self-select for participation, those with high educational attainment, and often those with relatively strong English language skills. Consequently, some older adults experiencing linguistic or cultural barriers, cognitive or sensory impairments, or other intersecting disadvantages were underrepresented. Future work might incorporate more targeted outreach and co-design strategies to ensure representation of the high-risk groups that the preliminary findings identified.

7.4 Implications for policy and practice

7.4.1 Greater representation of the unique needs and experiences of older adults in the Online Safety Act 2023 Bill.

A central element of the Online Safety Act (2023) Bill is the protection of children and young people. User-to-user services are mandated, for example, to conduct and publish risk assessments for child users, implement age verification measures, and maintain specific

safeguards for content likely to be harmful to children. Such provisions are not mirrored with regards to older adults, despite the association of old age with certain vulnerabilities such as social isolation, sensory conditions and physical and mental health issues. While the Bill's child-safety focus doesn't preclude platforms from assisting older users, the legislation does not single out older adults to the same degree or with similar rigour, and this is suggestive of a lack of acknowledgement or intent to address corporate digital ageism (Rosales et al., 2023). My research indicates that organisations within the FJN often inadequately account for the needs and vulnerabilities of older adults who suffer, report and/or recover from cybercrime victimisation. I propose a mandate for law-enforcement, financial institutions and social media websites to conduct a risk assessment on the safety of older adults using their platforms, and to take proportionate measures relating to the design or operation of the service to: (a) protect older adults from cybercrime victimisation; (b) minimise the length and difficulty of cybercrime reporting processes for older adults; (c) communicate any processes or outcomes with respect and empathy and in consideration of different technological capabilities.

7.4.2 Consideration of cybercrime in the Police Race Action Plan

The Police Race Action Plan (College of Policing & NPCC, 2022) sets out changes across policing to improve outcomes for Black people who work within or interact with policing in the UK. Workstream 4 of the plan is entitled 'A police service that protects Black people from crime and seeks justice for Black people'. It proposes increased efforts to address crime types for which Black people suffer disproportionate rates of victimisation, in particular knife crime and homicide. In light of my finding that people of Black or mixed and multiple ethnicity are at greater risk of cybercrime, I recommend that any future versions communicate a need for greater exploration and analysis of this issue by police research and analysis functions, not solely through desk-based investigation but also outreach initiatives in order to gain a deep understanding of Black people's cybercrime victimisation experiences, with the aim of developing tailored interventions.

7.4.3 Incorporation of cybercrime and fraud victimisation information into guidance and/or training for health and social care professionals

My CSEW analysis showed that poor mental and physical health was associated with cybercrime victimisation. Indeed, Burton et al. (2022) theorise that poor mobility translates to higher online visibility and data sharing, whilst cognitive deficits and slower processing weaken one's financial literacy and ability to evaluate choices under time constraints, thus creating more opportunities for offenders and revictimization. Accordingly, I suggest that health and social care professionals should be equipped with the knowledge to recognise cybercrime victimisation warning signs and provide informed advice on how to report and recover from victimisation. To my knowledge, the only 'cybercrime victimisation warning signs' guidance that exists is that of Independent Age (2020). Such a list should be developed for use by health and social care professionals following expert consultation. Guidance on reporting and recovery options might be incorporated into existing guidance (e.g. BMA, 2024) around adults at risk, confidentiality and disclosure of information to other authorities.

7.4.4 Practical recommendations for increasing cybercrime reporting among older adults

Study 3's proposed activities and activity components to increase cybercrime reporting by older adults, presented in Table 5.2, represent research-informed practices that can be adopted by any number of FJN organisations or support charities. They aim to increase reporting of, reduce the chances of, and mitigate the harm associated with cybercrime victimisation and repeat victimisation among older adults.

7.5 Future research

There are several areas where I consider it would be beneficial to build on the insights into cybercrime risk factors, barriers to reporting and possible interventions presented here.

7.5.1 Expanding data collection methods

In this thesis, the traditional surveys, interview and workshop methods have been instrumental in capturing older adults' experiences of cybercrime. However, emerging digital tools and observational techniques could provide richer, more objective insights into online behaviours and vulnerabilities. Ethnographic studies such as that of Greenhalgh et al., (2015) who visited 40 older adults in their homes in order to inform the development of assisted living technologies, could offer valuable insights into how older adults navigate the digital technology. By observing real-time interactions, such as how they respond to suspicious messages or seek advice from others, researchers could better understand the social and cognitive processes that influence their online behaviour. Similarly, controlled phishing simulations could help identify key moments where users either recognise or fall victim to scams, providing crucial information for designing targeted interventions.

7.5.2 Engaging with ex-offenders

Much of the current research focuses on the experiences of older victims and the perspectives of professionals working in crime or health and social care. As discussed, a deeper understanding of how cybercrime offenders operate could be gained by involving them directly in future studies. Individuals who have engaged in online fraud, particularly those who have served sentences or exited cybercriminal networks, could provide invaluable insights into the methods they use to identify and manipulate older victims. Furthermore, ex-offenders could help uncover weaknesses in current prevention measures, identifying gaps in cybersecurity advice, reporting mechanisms, and victim support services that they have previously exploited.

7.5.3 Reaching under-served groups

Although this research has highlighted valuable perspectives of older adults, certain groups remain under-represented. Those with limited digital literacy, individuals from non-English-

speaking backgrounds, people living in rural communities, and residents of care homes may face unique vulnerabilities that have yet to be fully explored. To address this, future research might adopt more inclusive recruitment strategies. Partnering with community organisations and faith groups could help researchers connect with older adults who might not otherwise be aware of participation opportunities. Offering multilingual resources and culturally tailored cybersecurity training could also improve engagement and ensure that interventions resonate with diverse populations. Additionally, research methodologies should be adapted to meet the needs of under-served groups. Offline and hybrid approaches, such as in-person interviews, postal surveys, and telephone-based discussions could be used alongside digital methods to reach those with limited internet access. Providing accessible research materials, such as large-print, easy-read, or audio-based resources would further improve inclusivity and participation.

7.6 Conclusions

This thesis illuminates the underexplored issue of cybercrime among older adults and proposes practical solutions to address both prevention and barriers to reporting. Firstly, quantitative analysis of CSEW data suggested that while older age groups often have lower rates of online engagement, they are more likely to experience repeat cyber victimisation and suffer financial loss. The data confirmed the complexity of older adults' risk factors: health conditions, sex and ethnicity, among others, were associated with victimisation. Qualitative interviews and stakeholder discussions revealed how digital ageism impedes older adults from seeking help, a pattern further complicated by unfamiliar or demanding reporting processes.

These findings have important theoretical relevance. They refine the Routine Activities Approach by highlighting that less time online does not inherently reduce risk if safeguards or 'guardianship' are weak. In addition, the sense of shame and self-doubt evident among some participants aligns with Shattered Assumptions theory, showing how cyber victimisation can undermine older adults' sense of self-worth and trust in previously reliable institutions, and is

suggestive of what I propose to be ‘tertiary victimisation’. Meanwhile, the concept of digital ageism – where older people internalise negative societal stereotypes about their digital ability and corporate organisations do not actively consider the needs of older adults in the product and service design (Rosales et al., 2023) – emerges as a key influence in non-disclosure, underlining that practical cyber skills alone cannot solve the problem unless negative biases and self-blame are addressed.

In terms of implications, this thesis provides robust evidence that interventions must be multi-layered, combining awareness and confidence-building with structural changes in how older victims receive support. Immediate priorities include ensuring more empathetic and efficient reporting channels in order to mitigate secondary victimisation, training frontline staff to avoid victim-blaming, and promoting a culture of cybercrime awareness within health and social care settings. The proposed Online Porcupine model offers a tangible way to deliver support: group-based, social sessions that demystify cyber threats, normalise victim experiences, and provide step-by-step advice for reporting incidents. In emphasising the social dimension of cyber protection, the thesis moves beyond conventional (but also important) cyber-literacy programmes (e.g. Miller et al., 2024) to address themes such as embarrassment, denial and mistrust, while fostering closer collaboration among banks, police, community groups, and care practitioners. Moving forward, additional research is needed to further develop interventions like Online Porcupine alongside stakeholders and to evaluate their effectiveness in different environments – particularly among minority ethnic communities or those with limited English proficiency, where barriers to reporting may be compounded by language and cultural factors.

References

- Abdelhamid, M. (2020). The Role of Health Concerns in Phishing Susceptibility: Survey Design Study. *Journal of Medical Internet Research*, 22(5), e18394. <https://doi.org/10.2196/18394>
- ACAS. (2024, November 15). *Victimisation—Discrimination at work*. Advisory, Conciliation and Arbitration Service. <https://www.acas.org.uk/discrimination-and-the-law/victimisation>
- Action Fraud. (2019a). *Data sharing*. <https://www.actionfraud.police.uk/data-sharing>
- Action Fraud. (2019b). *Fraud and cyber crime statistics*. <https://www.actionfraud.police.uk/fraud-stats>
- Action Fraud. (2019c). *Victim resources*. Action Fraud. <https://www.actionfraud.police.uk/victim-resources>
- Action Fraud. (2019d). *What is Action Fraud?* Action Fraud. <https://www.actionfraud.police.uk/what-is-action-fraud>
- Action Fraud. (2020, September 10). *Bank branch staff and police team up to stop £19 million of fraud in first half of 2020*. Action Fraud. <https://www.actionfraud.police.uk/news/bank-branch-staff-and-police-team-up-to-stop-19-million-of-fraud-in-first-half-of-2020>
- Action Fraud. (2024, October 1). *Action Fraud: Stay safe online after £1.4 million lost from email and social media account hacking in the last year*. <https://www.actionfraud.police.uk/news/socialmediahacking>
- Age UK. (2018). *Applying the brakes: Slowing and stopping fraud against older people*. https://www.ageuk.org.uk/siteassets/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf
- Age UK. (2020, July 21). *What is frailty?* Age UK. <https://www.ageuk.org.uk/our-impact/policy-research/frailty-in-older-people/understanding-frailty/>
- Age UK. (2022). *Digital Buddies*. Age UK East London. <https://www.ageuk.org.uk/eastlondon/get-involved/volunteer/digital-buddies/>

- Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency. *Criminology*, 30(1), 47–88. <https://doi.org/10.1111/j.1745-9125.1992.tb01093.x>
- Ahmad, N. A., Abd Rauf, M. F., Mohd Zaid, N. N., Zainal, A., Tengku Shahdan, T. S., & Abdul Razak, F. H. (2022). Effectiveness of Instructional Strategies Designed for Older Adults in Learning Digital Technologies: A Systematic Literature Review. *SN Computer Science*, 3(2), 130. <https://doi.org/10.1007/s42979-022-01016-0>
- Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, 30(6), 1665–1687. <https://doi.org/10.1108/INTR-10-2019-0400>
- Alonso Berbotto, A., & Chainey, S. (2021). Theft of oil from pipelines: An examination of its crime commission in Mexico using crime script analysis. *Global Crime*, 22(4), 265–287. <https://doi.org/10.1080/17440572.2021.1925552>
- Alzheimer's Society. (2023). *What is mild cognitive impairment (MCI)?* (No. Factsheet 470).
- Alzheimers.gov. (2024, July). *What Is Mild Cognitive Impairment?* <http://www.nia.nih.gov/alzheimers-dementias/mild-cognitive-impairment>
- APA. (2013). *Trauma*. American Psychological Association. <https://www.apa.org/topics/trauma>
- APA. (2020, February 1). *Building your resilience*. <https://www.apa.org/topics/resilience/building-your-resilience>
- Aplin, R., Wiener, C., Proudman, C., Colley, S., Gladman, A., Fleming, J., Brown, J., Findlay, J., Allnock, D., Wager, N., QPM, D., Havers, B., & Tripathi, K. (2024). *Policing Public Protection: A Companion Guide*.
- Aransiola, J. O., & Asindemade, S. O. (2011). Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. <https://doi.org/10.1089/cyber.2010.0307>
- Arthur, A., Savva, G. M., Barnes, L. E., Borjian-Boroojeny, A., Dening, T., Jagger, C., Matthews, F. E., Robinson, L., & Brayne, C. (2019). Changing prevalence and treatment of depression among

- older people over two decades. *The British Journal of Psychiatry*, 216(1), 49–54.
<https://doi.org/10.1192/bjp.2019.193>
- Association for Real Change. (2013). *Mate Crime: A Challenge for Providers*. ARC Ltd.
<https://arcengland.org.uk/wp-content/uploads/2024/06/RCC-Mate-Crime-SCP.pdf>
- Awan, I., & Zempi, I. (2016). The affinity between online and offline anti-Muslim hate crime: Dynamics and impacts. *Aggression and Violent Behavior*, 27, 1–8.
<https://doi.org/10.1016/j.avb.2016.02.001>
- Azam, N. A., Buja, A. G., Ahmad, R., Latip, S. F. A., & Sahri, N. M. (2024). An Analysis of the Deployment of Synergistic Cyber Security Awareness Model for the Elderly (SCSAM-Elderly) in Malaysia. *Akademika*, 94(3), 90–107. <https://doi.org/10.17576/akad-2024-9403-06>
- Bandura, A., & Walters, R. H. (with Internet Archive). (1963). *Social learning and personality development*. New York, Holt, Rinehart and Winston.
<http://archive.org/details/sociallearningpe00bandrich>
- Baron-Cohen, S., Richler, J., Bisarya, D., Gurnathan, N., & Wheelwright, S. (2003). The systemizing quotient: An investigation of adults with Asperger syndrome or high-functioning autism, and normal sex differences. *Philosophical Transactions of the Royal Society of London. Series B: Biological Sciences*, 358(1430), 361–374. <https://doi.org/10.1098/rstb.2002.1206>
- Beauregard, E. D., Rossmo, K., & Proulx, J. (2011). A Descriptive Model of the Hunting Process of Serial Sex Offenders: A Rational Choice Perspective. In *Crime Opportunity Theories*. Routledge.
- Beccaria, C. (2016). *On Crimes and Punishments*. Transaction Publishers.
- Beech, S. (2024, December 18). *Researchers uncover how cybercrime hits older adults harder*.
<https://www.msn.com/en-us/health/wellness/researchers-uncover-how-cybercrime-hits-older-adults-harder/ar-AA1w6HKN?ocid=Peregrine>

- Benbow, S. M., Bhattacharyya, S., Kingston, P., & Peisah, C. (2022). Invisible and at-risk: Older adults during the COVID-19 pandemic. *Journal of Elder Abuse & Neglect*, 34(1), 70–76.
<https://doi.org/10.1080/08946566.2021.2016535>
- Benetti-McQuoid, J., & Bursik, K. (2005). Individual Differences in Experiences of and Responses to Guilt and Shame: Examining the Lenses of Gender and Gender Role. *Sex Roles*, 53(1), 133–142. <https://doi.org/10.1007/s11199-005-4287-4>
- Bentham, J. (1781). An Introduction to the Principles of Morals and Legislation. *History of Economic Thought Books*. <https://ideas.repec.org//b/hay/hetboo/bentham1781.html>
- Bergmann, M. C., Dreißigacker, A., Skarczynski, B., von, & Rosa, W. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*. <https://doi.org/10.1089/cyber.2016.0727>
- Bernburg, J. G., & Krohn, M. D. (2003). Labeling, Life Chances, and Adult Crime: The Direct and Indirect Effects of Official Intervention in Adolescence on Crime in Early Adulthood. *Criminology*, 41(4), 1287–1318. <https://doi.org/10.1111/j.1745-9125.2003.tb01020.x>
- Bernet, A. C., Willens, D. E., & Bauer, M. S. (2013). Effectiveness-implementation hybrid designs: Implications for quality improvement science. *Implementation Science*, 8(1), S2.
<https://doi.org/10.1186/1748-5908-8-S1-S2>
- Betlej, A. (2023). Social Networks, New Technologies, and Wellbeing—An Interview Study on Factors Influencing Older Adults’ Successful Ageing. *International Journal of Environmental Research and Public Health*, 20(7), Article 7. <https://doi.org/10.3390/ijerph20075279>
- Bibbins-Domingo, K., & Helman, A. (2022). Why Diverse Representation in Clinical Research Matters and the Current State of Representation within the Clinical Research Ecosystem. In *Improving Representation in Clinical Trials and Research: Building Research Equity for Women and Underrepresented Groups*. National Academies Press (US).
<https://www.ncbi.nlm.nih.gov/books/NBK584396/>

- Biggane, A. M., Olsen, M., & Williamson, P. R. (2019). PPI in research: A reflection from early stage researchers. *Research Involvement and Engagement*, 5(1), 35.
<https://doi.org/10.1186/s40900-019-0170-2>
- Bishop, S. R., Lau, M., Shapiro, S., Carlson, L., Anderson, N. D., Carmody, J., Segal, Z. V., Abbey, S., Speca, M., Velting, D., & Devins, G. (2004). Mindfulness: A proposed operational definition. *Clinical Psychology: Science and Practice*, 11(3), 230–241.
<https://doi.org/10.1093/clipsy.bph077>
- Bisson, J. I., & Deahl, M. P. (1994). Psychological Debriefing and Prevention of Post-Traumatic Stress: More Research is Needed. *The British Journal of Psychiatry*, 165(6), 717–720.
<https://doi.org/10.1192/bjp.165.6.717>
- BMA. (2024, June). *Adults at risk, confidentiality and disclosure of information*. The British Medical Association. <https://www.bma.org.uk/advice-and-support/ethics/safeguarding/adults-at-risk-confidentiality-and-disclosure-of-information>
- Bone, J. K., Bu, F., Fluharty, M. E., Paul, E., Sonke, J. K., & Fancourt, D. (2022). Engagement in leisure activities and depression in older adults in the United States: Longitudinal evidence from the Health and Retirement Study. *Social Science & Medicine*, 294, 114703.
<https://doi.org/10.1016/j.socscimed.2022.114703>
- Borwell, J., Jansen, J., & Stol, W. (2022). The Psychological and Financial Impact of Cybercrime Victimization: A Novel Application of the Shattered Assumptions Theory. *Social Science Computer Review*, 40(4), 933–954. <https://doi.org/10.1177/0894439320983828>
- Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, 38(3), 227–236. <https://doi.org/10.1016/j.jcrimjus.2010.03.001>
- Bowers, K. J., & Guerette, R. T. (2014). Effectiveness of Situational Crime Prevention. In *Encyclopedia of Criminology and Criminal Justice* (pp. 1318–1329). Springer, New York, NY.
https://doi.org/10.1007/978-1-4614-5690-2_553

- Boyle, P. A., Yu, L., Wilson, R. S., Gamble, K., Buchman, A. S., & Bennett, D. A. (2012a). Poor Decision Making Is a Consequence of Cognitive Decline among Older Persons without Alzheimer's Disease or Mild Cognitive Impairment. *PLOS ONE*, 7(8), e43647.
<https://doi.org/10.1371/journal.pone.0043647>
- Boyle, P. A., Yu, L., Wilson, R. S., Gamble, K., Buchman, A. S., & Bennett, D. A. (2012b). Poor Decision Making Is a Consequence of Cognitive Decline among Older Persons without Alzheimer's Disease or Mild Cognitive Impairment. *PLOS ONE*, 7(8), e43647.
<https://doi.org/10.1371/journal.pone.0043647>
- Brantingham, P., & Brantingham, P. (2008). Crime pattern theory. In *Environmental Criminology and Crime Analysis*. Willan.
- Braun, V., & and Clarke, V. (2023). Toward good practice in thematic analysis: Avoiding common problems and be(com)ing a knowing researcher. *International Journal of Transgender Health*, 24(1), 1–6. <https://doi.org/10.1080/26895269.2022.2129597>
- Braz, C., & Robert, J.-M. (2006). Security and usability: The case of the user authentication methods. *Proceedings of the 18th Conference on l'Interaction Homme-Machine*, 199–203.
<https://doi.org/10.1145/1132736.1132768>
- Breen, C., Herley, C., & Redmiles, E. M. (2022). A Large-Scale Measurement of Cybercrime Against Individuals. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–41. <https://doi.org/10.1145/3491102.3517613>
- Brenner, S. (2007). *Cybercrime: Re-Thinking Crime Control Strategies (From Crime Online, P 12-28, 2007, Yvonne Jewkes, ed. —See NCJ-218881) | Office of Justice Programs*. US Department of Justice. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/cybercrime-re-thinking-crime-control-strategies-crime-online-p-12>
- Brunton-Smith, I. (2017). Fear 2.0: Worry about cybercrime in England and Wales. In *The Routledge International Handbook on Fear of Crime*. Routledge.

- Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, 159, 111678. <https://doi.org/10.1016/j.exger.2021.111678>
- Busaidi, Z. Q. A. (2010). The Concept of Somatisation: A Cross-cultural perspective. *Sultan Qaboos University Medical Journal*, 10(2), 180.
- Butler, R. N. (1969). Age-ism: Another Form of Bigotry. *The Gerontologist*, 9(4 Part 1), 243–246. https://doi.org/10.1093/geront/9.4_Part_1.243
- Butler, R. N. (1980). Ageism: A Foreword. *Journal of Social Issues*, 36(2), 8–11. <https://doi.org/10.1111/j.1540-4560.1980.tb02018.x>
- Button, M., Shepherd, D. W. J., Hawkins, C. D., & Tapley, J. (2024). Disseminating fraud awareness and prevention advice to older adults: Perspectives on the most effective means of delivery. *Crime Prevention and Community Safety*. <https://doi.org/10.1057/s41300-024-00218-3>
- Cabinet Office. (2011). *The Cost of Cybercrime*. GOV.UK. <https://www.gov.uk/government/publications/the-cost-of-cyber-crime-joint-government-and-industry-report>
- Cambridge Dictionary. (2024, November 27). *Scam*. <https://dictionary.cambridge.org/dictionary/english/scam>
- Carminati, J.-Y. J., Ponsford, J. L., & Gould, K. R. (2023). “This group... I felt like I was medicating myself from this cyberscam illness that was living with me.” A qualitative evaluation of co-designing cybersafety training resources with and for people with acquired brain injury. *Disability and Rehabilitation*, 45(22), 3719–3729. <https://doi.org/10.1080/09638288.2022.2139418>
- Carnall Farrar. (2024). *The Economic Impact of Dementia*. <https://www.alzheimers.org.uk/sites/default/files/2024-05/the-annual-costs-of-dementia.pdf>
- Ceccato, V. A. (2016). *Rural Crime and Community Safety*. <https://doi.org/10.4324/9780203725689>

- Chan, J., & Bennett Moses, L. (2016). Is Big Data challenging criminology? *Theoretical Criminology*, 20(1), 21–39. <https://doi.org/10.1177/1362480615586614>
- Chawla, K., Kunonga, T. P., Stow, D., Barker, R., Craig, D., & Hanratty, B. (2021). Prevalence of loneliness amongst older people in high-income countries: A systematic review and meta-analysis. *PLOS ONE*, 16(7), e0255088. <https://doi.org/10.1371/journal.pone.0255088>
- Cho, S., Crenshaw, K. W., & McCall, L. (2013). Toward a Field of Intersectionality Studies: Theory, Applications, and Praxis. *Signs: Journal of Women in Culture and Society*, 38(4), 785–810. <https://doi.org/10.1086/669608>
- Choi, E., Park, N., Lutze, F. E., & Neuilly, M.-A. (2021). How Do Victims of Sexual Violence Benefit From Mutual Disclosure? An Exploratory Study of Women in South Korea. *Journal of Interpersonal Violence*, 36(9–10), 4641–4667. <https://doi.org/10.1177/0886260518789145>
- Choi, N. G., Kulick, D. B., & Mayer, J. (1999). Financial Exploitation of Elders: Analysis of Risk Factors Based on County Adult Protective Services Data. *Journal of Elder Abuse & Neglect*, 10(3–4), 39–62. https://doi.org/10.1300/J084v10n03_03
- Choudrie, J., Pheeraphuttrangkoon, S., & Davari, S. (2020). The Digital Divide and Older Adult Population Adoption, Use and Diffusion of Mobile Phones: A Quantitative Study. *Information Systems Frontiers*, 22(3), 673–695. <https://doi.org/10.1007/s10796-018-9875-2>
- City of London Police. (2023a, June 13). *New suppliers appointed for Action Fraud service replacement*. <https://www.cityoflondon.police.uk/news/city-of-london/news/2023/june/new-suppliers-appointed-for-action-fraud-service-replacement/>
- City of London Police. (2023b, November 22). *National Policing Strategy for Fraud, Economic and Cyber Crime 2023-2028*. https://www.cityoflondon.police.uk/SysSiteAssets/media/downloads/city-of-london/about-us/colp_national-policing-strategy-document.pdf
- Cjaza, R., Blair, J., & Eastman, E. (1994). Respondent Strategies for Recall of Crime Victimization Incidents—ProQuest. *Journal of Official Statistics*, 10(3).

<https://www.proquest.com/openview/3736928e1c90941d2f719e76862de057/1?pq-origsite=gscholar&cbl=105444>

Clarke, R. V. (2017). Chapter 13 Situational Crime Prevention. In *Environmental Criminology and Crime Analysis*.

Clarke, R. V., & Eck, J. E. (2003). *Becoming a problem solving crime analyst: In 55 small steps*. Jill Dando Institute of Crime Science, University College London.

Code of Practice for Victims of Crime in England and Wales. (2020, November). Ministry of Justice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/936239/victims-code-2020.pdf

Cohen, A. K. (1955). *DELINQUENT BOYS: THE CULTURE OF THE GANG*.

<https://www.ojp.gov/ncjrs/virtual-library/abstracts/delinquent-boys-culture-gang>

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>

Cole, R. (2024). A qualitative investigation of the emotional, physiological, financial, and legal consequences of online romance scams in the United States. *Journal of Economic Criminology*, 6, 100108. <https://doi.org/10.1016/j.jeconc.2024.100108>

College of Policing, & NPCC. (2022). *Police Race Action Plan*. <https://www.college.police.uk/support-forces/diversity-and-inclusion/action-plan>

Collins English Dictionary. (2024). *VICTIMIZE definition and meaning*.

<https://www.collinsdictionary.com/dictionary/english/victimize>

Collins English Dictionary. (2025). *VICTIMHOOD definition and meaning*. Collins English Dictionary.

<https://www.collinsdictionary.com/dictionary/english/victimhood>

Cooper, C., Bebbington, P., McManus, S., Meltzer, H., Stewart, R., Farrell, M., King, M., Jenkins, R., & Livingston, G. (2010). The treatment of Common Mental Disorders across age groups:

Results from the 2007 Adult Psychiatric Morbidity Survey. *J Affect Disord*, 127(1–3), 96–101.

<https://doi.org/10.1016/j.jad.2010.04.020>

- Cooper, C., Mansour, H., Carter, C., Rapaport, P., Morgan-Trimmer, S., Marchant, N., Poppe, M., Higgs, P., Brierley, J., Solomon, N., Budgett, J., Bird, M., Walters, K., Barber, J., Wenborn, J., Lang, I., Huntley, J., Ritchie, K., Kales, H., ... Palomo, M. (2021). Social connectedness and dementia prevention: Pilot of the APPLE-Tree video-call intervention during the Covid-19 pandemic. *Dementia*, 14713012211014382–14713012211014382.
<https://doi.org/10.1177/14713012211014382>
- Cornish, D. B., & Clarke, R. V. (2017). The Rational Choice Perspective. In *Environmental Criminology and Crime Analysis* (Kindle, pp. 29–61). Routledge.
- Correia, S. G. (2022). Making the most of cybercrime and fraud crime report data: A case study of UK Action Fraud. *International Journal of Population Data Science*, 7(1), 1721.
<https://doi.org/10.23889/ijpds.v7i1.1721>
- Cortina, L. M., Rabelo, V. C., & Holland, K. J. (2018). Beyond Blaming the Victim: Toward a More Progressive Understanding of Workplace Mistreatment. *Industrial and Organizational Psychology*, 11(1), 81–100. <https://doi.org/10.1017/iop.2017.54>
- Cotti, A., Magalhaes, T., Pinto da Costa, D., & Matos, E. (2004). Road Traffic Accidents and Secondary Victimization: The Role of Law Professionals Medical Law. *Medicine and Law*, 23(2), 259–268.
- CPS. (2018, May 1). *Cybercrime—Prosecution guidance*. The Crown Prosecution Service.
<https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>
- CPS. (2022a). *Fraud and economic crime*. The Crown Prosecution Service.
<https://www.cps.gov.uk/crime-info/fraud-and-economic-crime>
- CPS. (2022b). *Hate crime*. The Crown Prosecution Service. <https://www.cps.gov.uk/crime-info/hate-crime>
- Cross, C. (2013). “Nobody’s holding a gun to your head...”: Examining current discourses surrounding victims of online fraud. In J. Tauri & K. Richards (Eds.), *Crime, Justice and Social Democracy: Proceedings of the 2nd International Conference, 2013, Volume 1* (pp. 25–32). Crime, Justice

- and Social Democracy International Conference, Australia. Crime and Justice Research Centre, Queensland University of Technology. <http://crimejusticeconference.com/>
- Cross, C. (2019). Who is to blame? Exploring accountability in fraud victimisation. *Journal of Criminological Research, Policy and Practice*, 6(1), 35–48. <https://doi.org/10.1108/JCRPP-07-2019-0054>
- Cross, C. (2021). Theorising the impact of COVID-19 on the fraud victimisation of older persons. *The Journal of Adult Protection*, 23(2), 98–109. <https://doi.org/10.1108/JAP-08-2020-0035>
- Cross, C., & Richards, K. (2015). The ‘ACA Effect’: Examining How Current Affairs Programs Shape Victim Understandings and Responses to Online Fraud. *Current Issues in Criminal Justice*, 27(2), 163–178. <https://doi.org/10.1080/10345329.2015.12036039>
- Cuibus, M. (2024, August 9). *Migrants in the UK: An Overview*. Migration Observatory. <https://migrationobservatory.ox.ac.uk/resources/briefings/migrants-in-the-uk-an-overview/>
- Dancig-Rosenberg, H., & Yosef, N. (2019). Crime Victimhood and Intersectionality. *Fordham Urban Law Journal*, 47(1), 85–116.
- Darby, R. R., & Dickerson, B. C. (2017). Dementia, Decision Making, and Capacity. *Harvard Review of Psychiatry*, 25(6), 270. <https://doi.org/10.1097/HRP.0000000000000163>
- De Silva, M. J., Breuer, E., Lee, L., Asher, L., Chowdhary, N., Lund, C., & Patel, V. (2014). Theory of Change: A theory-driven approach to enhance the Medical Research Council’s framework for complex interventions. *Trials*, 15(1), 267. <https://doi.org/10.1186/1745-6215-15-267>
- DeCamp, W., & Zaykowski, H. (2015). Developmental victimology: Estimating group victimization trajectories in the age–victimization curve. *International Review of Victimology*, 21(3), 255–272. <https://doi.org/10.1177/0269758015591722>
- Delello, J. A., & McWhorter, R. R. (2017). Reducing the Digital Divide: Connecting Older Adults to iPad Technology. *Journal of Applied Gerontology*, 36(1), 3–28. <https://doi.org/10.1177/0733464815589985>

- DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2017). *Exploring the Risks and Consequences of Elder Fraud Victimization: Evidence from the Health and Retirement Study* (SSRN Scholarly Paper No. 3124952). <https://doi.org/10.2139/ssrn.3124952>
- Delker, B. C., Salton, R., & McLean, K. C. (2020). Giving Voice to Silence: Empowerment and Disempowerment in the Developmental Shift from Trauma 'Victim' to 'Survivor-Advocate.' *Journal of Trauma & Dissociation*, 21(2), 242–263.
<https://doi.org/10.1080/15299732.2019.1678212>
- DeNicola, L. (2024, April 17). *The 10 Most Common Types of Fraud*. Experian.
<https://www.experian.com/blogs/ask-experian/most-common-types-of-fraud/>
- Department for Science, Innovation & Technology. (2024a). *Cyber security breaches survey 2024*.
<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024>
- Department for Science, Innovation & Technology. (2024b, January 23). *Cyber Governance Code of Practice: Call for views*. GOV.UK. <https://www.gov.uk/government/calls-for-evidence/cyber-governance-code-of-practice-call-for-views/cyber-governance-code-of-practice-call-for-views>
- Dias, I., & Fraga, S. (2024). "Older people are weak": Perceptions and meanings of ageing and abuse against older people. *Frontiers in Sociology*, 8, 1329005.
<https://doi.org/10.3389/fsoc.2023.1329005>
- Dodgson, J. E. (2019). Reflexivity in Qualitative Research. *Journal of Human Lactation*, 35(2), 220–222. <https://doi.org/10.1177/0890334419830990>
- DofE. (2022, March 18). *Volunteering ideas for under 16s*. The Duke of Edinburgh's Award.
<https://www.dofe.org/thelatest/volunteering-ideas/>
- DofE. (2024, March 10). *Volunteering ideas for under 16s*. The Duke of Edinburgh's Award.
<https://www.dofe.org/thelatest/volunteering-ideas/>

- Doherty, G. (2015). Do mates hate? A framing of the theoretical position of mate crime and an assessment of its practical impact. *The Journal of Adult Protection*, 17(5), 296–307.
<https://doi.org/10.1108/JAP-12-2014-0041>
- Draper, H., & Sorell, T. (2013). telecare, Remote Monitoring and Care. *Bioethics*, 27(7), 365–372.
<https://doi.org/10.1111/j.1467-8519.2012.01961.x>
- Drisko, J. W. (2025). Transferability and Generalization in Qualitative Research. *Research on Social Work Practice*, 35(1), 102–110. <https://doi.org/10.1177/10497315241256560>
- Ehlert, C., & Rüdiger, T.-G. (2020). Defensible Digital Space. In T.-G. Rüdiger & P. S. Bayerl (Eds.), *Cyberkriminologie: Kriminologie für das digitale Zeitalter* (pp. 151–171). Springer Fachmedien. https://doi.org/10.1007/978-3-658-28507-4_6
- Elliott, I., Thomas, S., & Ogloff, J. (2014). Procedural justice in victim-police interactions and victims' recovery from victimisation experiences. *Policing and Society*, 24(5), 588–601.
<https://doi.org/10.1080/10439463.2013.784309>
- Erbach, M., Danseco, E., & Schutte, V. (2024). Evaluating a helpline for post-secondary students: Caller distress, ability to face concern and satisfaction with helpline. *Counselling and Psychotherapy Research*, 24(2), 829–841. <https://doi.org/10.1002/capr.12718>
- erfan, S. (2025, January 23). *What is the difference between a School, University, and College in the UK? - Blog*. <https://theproeducator.com/blog/school-university-and-college-in-the-uk/>,
<https://theproeducator.com/blog/school-university-and-college-in-the-uk/>
- Errol, Z., Madsen, J. B., & Moslehi, S. (2021). Social disorganization theory and crime in the advanced countries: Two centuries of evidence. *Journal of Economic Behavior & Organization*, 191, 519–537. <https://doi.org/10.1016/j.jebo.2021.09.017>
- Estebarsari, F., Dastoorpoor, M., Khalifehkandi, Z. R., Nouri, A., Mostafaei, D., Hosseini, M., Esmaeili, R., & Aghababaeian, H. (2020). The Concept of Successful Aging: A Review Article. *Current Aging Science*, 13(1), 4–10. <https://doi.org/10.2174/1874609812666191023130117>

- European Commission. (2007, May 22). *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions—Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642}*. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267>
- European Institute for Gender Equality. (2024, December 10). *Secondary victimisation* /. https://eige.europa.eu/publications-resources/thesaurus/terms/1248?language_content_entity=en
- Fader, J. J., & León, K. S. (2024). Code of the Street 25 Years Later: Lasting Legacies, Empirical Status, and Future Directions. *Annual Review of Criminology*, 7(Volume 7, 2024), 19–38. <https://doi.org/10.1146/annurev-criminol-022422-123641>
- Farage, M. A., Miller, K. W., Ajayi, F., & Hutchins, D. (2012). Design Principles to Accommodate Older Adults. *Global Journal of Health Science*, 4(2), 2–25. <https://doi.org/10.5539/gjhs.v4n2p2>
- Farrell, G., & Pease, K. (2017). Repeat Victimisation. In R. Wortley (Ed.), *Environmental Criminology and Crime Analysis* (Kindle Edition, pp. 180–198). Taylor and Francis.
- Felson, M. (2017). The routine activity approach. In *Environmental Criminology and Crime Analysis* (Kindle, pp. 87–97). Routledge.
- Feng, Z., Lugtenberg, M., Franse, C., Fang, X., Hu, S., Jin, C., & Raat, H. (2017). Risk factors and protective factors associated with incident or increase of frailty among community-dwelling older adults: A systematic review of longitudinal studies. *PLOS ONE*, 12(6), e0178383. <https://doi.org/10.1371/journal.pone.0178383>
- Fine, B. (1977). Labelling theory: An investigation into the sociological critique of deviance. *Economy and Society*, 6(2), 166–193. <https://doi.org/10.1080/030851477000000003>
- Fineman, M. A. (2010). The Vulnerable Subject and the Responsive State The 2010 Randolph W. Thrower Symposium: The New New Deal: From De-Regulation to Re-Regulation. *Emory Law Journal*, 60(2), 251–276.

- Finlay, L. (2002). Negotiating the swamp: The opportunity and challenge of reflexivity in research practice. *Qualitative Research*, 2(2), 209–230.
<https://doi.org/10.1177/146879410200200205>
- Fitzgerald, K. N., Campbell, T., Makarem, S., & Hodges, R. (2023). Potential reversal of biological age in women following an 8-week methylation-supportive diet and lifestyle program: A case series. *Aging*, 15(6), 1833–1839. <https://doi.org/10.18632/aging.204602>
- Fleck, A. (2024, February 22). *Infographic: Cybercrime Expected To Skyrocket in Coming Years*. Statista Daily Data. <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027>
- Follette, V. M., Palm, K. M., & Hall, M. L. R. (2004). Acceptance, Mindfulness, and Trauma. In *Mindfulness and acceptance: Expanding the cognitive-behavioral tradition* (pp. 192–208). The Guilford Press.
- Foster, L. (2018). Active Ageing, Pensions and Retirement in the UK. *Journal of Population Ageing*, 11(2), 117–132. <https://doi.org/10.1007/s12062-017-9181-7>
- Frese, T., Mahlmeister, J., Deutsch, T., & Sandholzer, H. (2016). Reasons for elderly patients GP visits: Results of a cross-sectional study. *Clinical Interventions in Aging*, 11, 127–132.
<https://doi.org/10.2147/CIA.S88354>
- Frothingham, S. (2019, February 15). *Chronological vs. Biological Aging: Differences & More*. Healthline. <https://www.healthline.com/health/chronological-ageing>
- FTC. (2024, October 11). *Malware: How To Protect Against, Detect, and Remove It*. Federal Trade Commission. <https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it>
- Furnell, S., & Dowling, S. (2019). Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, 5(1), 13–26. <https://doi.org/10.1108/JCRPP-07-2018-0021>

- Gale, N. K., Heath, G., Cameron, E., Rashid, S., & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology*, 13(1), 117. <https://doi.org/10.1186/1471-2288-13-117>
- Gámez-Guadix, M., Orue, I., Smith, P. K., & Calvete, E. (2013). Longitudinal and Reciprocal Relations of Cyberbullying With Depression, Substance Use, and Problematic Internet Use Among Adolescents. *Journal of Adolescent Health*, 53(4), 446–452. <https://doi.org/10.1016/j.jadohealth.2013.03.030>
- Garavaglia, E., Caliendo, A., Melis, G., Sala, E., & Zaccaria, D. (2023). Contrasting ageism in research on older adults and digital technologies: A methodological reflection. In *Digital Ageism*. Routledge.
- Garlicki, J., & Mider, D. (2022). Financial Cybercrimes in Poland – In the Search of Victimization Factors. *European Research Studies*, XXV(3), 299–313.
- Giles, H., & Reid, S. A. (2005). Ageism Across the Lifespan: Towards a Self-Categorization Model of Ageing. *Journal of Social Issues*, 61(2), 389–404. <https://doi.org/10.1111/j.1540-4560.2005.00412.x>
- Gilleard, C., & Higgs, P. (2010). Aging without agency: Theorizing the fourth age. *Aging & Mental Health*, 14(2), 121–128. <https://doi.org/10.1080/13607860903228762>
- Glassner, S. D. (2020). Bullying victimization and delinquent involvement: An application of general strain theory. *Children and Youth Services Review*, 116, 105099. <https://doi.org/10.1016/j.childyouth.2020.105099>
- Goodman, C., & Lambert, K. (2023). Scoping review of the preferences of older adults for patient education materials. *Patient Education and Counseling*, 108, 107591. <https://doi.org/10.1016/j.pec.2022.107591>
- Graham, A., Kulig, T. C., & Cullen, F. T. (2019). Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal*, 43(1), 1–16. <https://doi.org/10.1108/PIJPSM-07-2019-0115>

- Greenhalgh, T., Procter, R., Wherton, J., Sugarhood, P., Hinder, S., & Rouncefield, M. (2015). What is quality in assisted living technology? The ARCHIE framework for effective telehealth and telecare services. *BMC Medicine*, 13(1), 91. <https://doi.org/10.1186/s12916-015-0279-6>
- Griffiths, C. (2024, October 1). *The Latest Cyber Crime Statistics*. AAG. <https://aag-it.com/the-latest-cyber-crime-statistics/>
- Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, 4. <https://doi.org/10.3389/fdata.2021.583723>
- Gross, Y. (2020). Erikson's Stages of Psychosocial Development. In *The Wiley Encyclopedia of Personality and Individual Differences* (pp. 179–184). John Wiley & Sons, Ltd. <https://doi.org/10.1002/9781118970843.ch31>
- Haimi, M., & Sergienko, R. (2024). Adoption and Use of Telemedicine and Digital Health Services Among Older Adults in Light of the COVID-19 Pandemic: Repeated Cross-Sectional Analysis. *JMIR Aging*, 7(1), e52317. <https://doi.org/10.2196/52317>
- Halevi, T., Memon, N., & Nov, O. (2015). *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks* (SSRN Scholarly Paper No. 2544742). Social Science Research Network. <https://doi.org/10.2139/ssrn.2544742>
- Hasan, M. S., Rahman, R. A., Abdillah, S. F. H. B. T., & Omar, N. (2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11(4), 395–404. <https://doi.org/10.3844/jssp.2015.395.404>
- Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. (2024a). A qualitative study exploring factors preventing older adults from reporting cybercrime and seeking help. In *CrimRxiv*. <https://doi.org/10.21428/cb6ab371.8c4e3181>
- Havers, B., Tripathi, K., Burton, A., Martin, W., & Cooper, C. (2024b). Exploring the Factors Preventing Older Adults From Reporting Cybercrime and Seeking Help: A Qualitative,

- Semistructured Interview Study. *Health & Social Care in the Community*, 2024(1), 1314265.
<https://doi.org/10.1155/2024/1314265>
- Havers, B., Tripathi, K., Burton, A., McManus, S., & Cooper, C. (2024a). Cybercrime victimisation among older adults: A probability sample survey in England and Wales. *PLOS ONE*, 19(12), e0314380. <https://doi.org/10.1371/journal.pone.0314380>
- Havers, B., Tripathi, K., Burton, A., McManus, S., & Cooper, C. (2024b). Research Note: Cybercrime victimisation among older adults: a probability sample survey in England and Wales. In *CrimRxiv*. <https://doi.org/10.21428/cb6ab371.46d2b268>
- Hawks Jr, A., & McDonald-Lopez, K. (2021). Reestablishing the Foundations: Investigating the Theoretical and Practical Boundaries of Criminology. *International Journal of Social Science Research*, 10(1), Article 1. <https://doi.org/10.5296/ijssr.v10i1.19289>
- Haynie, D. L., & Osgood, D. W. (2005). Reconsidering Peers and Delinquency: How do Peers Matter? *Social Forces*, 84(2), 1109–1130. <https://doi.org/10.1353/sof.2006.0018>
- Helmbrecht, U. (2016). Cybersecurity for an Open, Safe and Secure Cyberspace in Europe. In C. Bär, A. T. Fischer, & H. Gulden (Eds.), *Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand: Festschrift für Professor Dieter Kempf* (pp. 91–100). Springer. https://doi.org/10.1007/978-3-662-44909-7_10
- Helweg-Larsen, K., Schütt, N., & Larsen, H. B. (2012). Predictors and protective factors for adolescent Internet victimization: Results from a 2008 nationwide Danish youth survey. *Acta Paediatrica*, 101(5), 533–539. <https://doi.org/10.1111/j.1651-2227.2011.02587.x>
- Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security Journal*, 26(4), 383–402.
<https://doi.org/10.1057/sj.2013.25>
- HM Treasury. (2024, October 3). *New powers for banks to combat fraudsters*. GOV.UK.
<https://www.gov.uk/government/news/new-powers-for-banks-to-combat-fraudsters>

- HMICFRS. (2021, February 18). *Regional Organised Crime Units: An inspection of the effectiveness of the Regional Organised Crime Units*. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. <https://hmicfrs.justiceinspectorates.gov.uk/publication-html/regional-organised-crime-units-effectiveness/>
- HMICFRS. (2023, May 9). *Vulnerable person*. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. <https://hmicfrs.justiceinspectorates.gov.uk/glossary/vulnerable-person/>
- Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review. *Computers & Security*, 115, 102611. <https://doi.org/10.1016/j.cose.2022.102611>
- Hodge, G. (2016). Suicide in an ageing UK population: Problems and prevention. *Quality in Ageing and Older Adults*, 17(4), 218–228. <https://doi.org/10.1108/QAOA-05-2015-0022>
- Home Office. (2022). *Home Office Counting Rules for Recorded Crime*. <https://www.gov.uk/government/publications/counting-rules-for-recorded-crime>
- Hoogendijk, E. O., Afilalo, J., Ensrud, K. E., Kowal, P., Onder, G., & Fried, L. P. (2019). Frailty: Implications for clinical practice and public health. *The Lancet*, 394(10206), 1365–1375. [https://doi.org/10.1016/S0140-6736\(19\)31786-6](https://doi.org/10.1016/S0140-6736(19)31786-6)
- Horowitz, M., Wilner, N., & Alvarez, W. (1979). Impact of Event Scale: A measure of subjective stress. *Psychosomatic Medicine*, 41(3), 209–218. <https://doi.org/10.1097/00006842-197905000-00004>
- Houtti, M., Roy, A., Gangula, V. N. R., & Walker, A. M. (2024). A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries. *Journal of Online Trust and Safety*. <https://doi.org/10.48550/arXiv.2407.12896>
- Hsu, J. W., & Willis, R. (2013). Dementia Risk and Financial Decision Making by Older Households: The Impact of Information. *Journal of Human Capital*, 7(4), 340–377. <https://doi.org/10.1086/674105>

- Hu, P., Wu, T. ting, Wu, C. bin, Huang, H., Fu, Z., Du, L., Xu, X. long, Shi, Z., & Zhao, Y. (2017). *Evaluation of “being healthy, being away from chronic diseases” public service advertisement in Chongqing, China: A cross-sectional study* (No. e2985v1). PeerJ Inc.
<https://doi.org/10.7287/peerj.preprints.2985v1>
- Hudgens, G. A., & Fatkin, L. T. (1985). Sex differences in risk taking: Repeated sessions on a computer-simulated task. *The Journal of Psychology: Interdisciplinary and Applied*, 119, 197–206. <https://doi.org/10.1080/00223980.1985.10542887>
- Hutchings, A., & Holt, T. J. (2018). *Interviewing cybercrime offenders*.
<https://doi.org/10.17863/CAM.24191>
- ICO. (2024a, July 19). *London Borough of Hackney reprimanded following cyber-attack*. Information Commissioner’s Office; ICO. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/london-borough-of-hackney-reprimanded-following-cyber-attack/>
- ICO. (2024b, November 19). *The role of the National Cyber Security Centre (NCSC)*. Information Commissioner’s Office; ICO. <https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/>
- ICO. (2024c, November 27). *Enforcement of this code*. ICO. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/enforcement-of-this-code/>
- Indepent Age. (2020). *How to help someone if you think they’re being scammed*.
<https://www.independentage.org/get-advice/money/scams/how-to-help-someone-if-you-think-theyre-being-scammed>
- Innes, A., Chesterton, L., Morris, L., Smith, S. K., & Bushell, S. (2022). Perspectives of people living with dementia and their care partners about the impact on social health when participating in a co-designed Dementia café. *Health & Social Care in the Community*, 30(4), e1375–e1383. <https://doi.org/10.1111/hsc.13545>

- Ioannou, M., Synnott, J., Reynolds, A., & Pearson, J. (2018). A comparison of online and offline Grooming characteristics: An application of the victim roles model. *Computers in Human Behavior*, 85, 291–297. <https://doi.org/10.1016/j.chb.2018.04.011>
- ISACA (Ed.). (2019). *State of Cybersecurity 2019*. ISACA. https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619
- Iversen, C., & Westerlund, M. (2024). Users' Perspectives on Crisis Helplines in Relation to Professional Mental Health Services. *Crisis*, 45(3), 173–179. <https://doi.org/10.1027/0227-5910/a000876>
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In J. Joseph & S. Jergenson (Eds.), *An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen* (pp. 3–19). Springer International Publishing. https://doi.org/10.1007/978-3-030-41622-5_1
- Janoff-Bulman, R. (1999). Rebuilding Shattered Assumptions after Traumatic Life Events: Coping Processes and Outcomes. In C. R. Snyder (Ed.), *Coping: The Psychology of What Works* (p. 0). Oxford University Press. <https://doi.org/10.1093/med:psych/9780195119343.003.0014>
- Jeffery, C. R. (1972). Crime Prevention Through Environmental Design. *Criminology*, 10(2), 191–191. <https://doi.org/10.1111/j.1745-9125.1972.tb00553.x>
- John, A., Saunders, R., Desai, R., Bell, G., Fearn, C., Buckman, J., Brown, B., Nurock, S., Michael, S., Ware, P., Marchant, N., Aguirre, E., Rio, M., Cooper, C., Pilling, S., Richards, M., & Stott, J. (2022). Associations between psychological therapy outcomes for depression and incidence of dementia. *Psychological Medicine*. <https://doi.org/10.1017/S0033291722002537>
- Johnson, S. (2017). Crime mapping and spatial analysis. In *Environmental Criminology and Crime Analysis* (Kindle, pp. 199–222). Routledge.
- Jones, G. M. M., & Miesen, B. M. L. (2004). *Care-Giving in Dementia V3: Research and Applications*. Routledge.

- Junger, M., Montoya, L., Hartel, P., & Heydari, M. (2017). Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. <https://doi.org/10.1109/CyberSA.2017.8073391>
- Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime Victimization and Subjective Well-Being: An Examination of the Buffering Effect Hypothesis Among Adolescents and Young Adults. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 129–137. <https://doi.org/10.1089/cyber.2016.0728>
- Kaakinen, M., Koivula, A., Savolainen, I., Sirola, A., Mikkola, M., Zych, I., Paek, H.-J., & Oksanen, A. (2021). Online dating applications and risk of youth victimization: A lifestyle exposure perspective. *Aggressive Behavior*, 47(5), 530–543. <https://doi.org/10.1002/ab.21968>
- Karagiannopoulos, Dr. V., Kirby, Dr. A., Oftadeh-Moghadam, S., & Sugiura, Dr. L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, 43, 105615. <https://doi.org/10.1016/j.clsr.2021.105615>
- Knöchel, C., Alves, G., Friedrichs, B., Schneider, B., Schmidt-Rechau, A., Wenzler, S., Schneider, A., Prvulovic, D., Carvalho, A. F., & Oertel-Knöchel, V. (2015). Treatment-resistant Late-life Depression: Challenges and Perspectives. *Current Neuropsychopharmacology*, 13(5), 577–591. <https://doi.org/10.2174/1570159x1305151013200032>
- Koning, L., Junger, M., & Veldkamp, B. (2023). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International Review of Victimology*, 02697580231215839. <https://doi.org/10.1177/02697580231215839>
- Kornadt, A. E., Albert, I., Hoffmann, M., Murdock, E., & Nell, J. (2021). Perceived Ageism During the Covid-19-Crisis Is Longitudinally Related to Subjective Perceptions of Aging. *Frontiers in Public Health*, 9. <https://doi.org/10.3389/fpubh.2021.679711>
- Kosinski, M. (2024, August 16). *What Is Hacking?* IBM. <https://www.ibm.com/topics/cyber-hacking>

- Kubrin, C. E. (2009). Social Disorganization Theory: Then, Now, and in the Future. In M. D. Krohn, A. J. Lizotte, & G. P. Hall (Eds.), *Handbook on Crime and Deviance* (pp. 225–236). Springer.
https://doi.org/10.1007/978-1-4419-0245-0_12
- Kung, C. S. J., & Steptoe, A. (2023). Changes in Internet use patterns among older adults in England from before to after the outbreak of the COVID-19 pandemic. *Scientific Reports*, 13(1), Article 1. <https://doi.org/10.1038/s41598-023-30882-8>
- Laing, L. (2017). Secondary Victimization: Domestic Violence Survivors Navigating the Family Law System. *Violence Against Women*, 23(11), 1314–1335.
<https://doi.org/10.1177/1077801216659942>
- Lasky, N. V. (2019). Victim Precipitation Theory. In *The Encyclopedia of Women and Crime* (pp. 1–2). John Wiley & Sons, Ltd. <https://doi.org/10.1002/9781118929803.ewac0517>
- Lee, C. C., Czaja, S. J., Moxley, J. H., Sharit, J., Boot, W. R., Charness, N., & Rogers, W. A. (2019). Attitudes Toward Computers Across Adulthood From 1994 to 2013. *The Gerontologist*, 59(1), 22–33. <https://doi.org/10.1093/geront/gny081>
- Lee, Y., Chi, I., & Palinkas, L. A. (2019). Retirement, Leisure Activity Engagement, and Cognition Among Older Adults in the United States. *Journal of Aging and Health*, 31(7), 1212–1234.
<https://doi.org/10.1177/0898264318767030>
- legislation.gov.uk. (2017). *The Payment Services Regulations*. Statute Law Database.
<https://www.legislation.gov.uk/uksi/2017/752/contents>
- Leitão, C., Mignano, A., Estrela, M., Fardilha, M., Figueiras, A., Roque, F., & Herdeiro, M. T. (2022). The Effect of Nutrition on Aging—A Systematic Review Focusing on Aging-Related Biomarkers. *Nutrients*, 14(3), Article 3. <https://doi.org/10.3390/nu14030554>
- Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263–280.
<https://doi.org/10.1080/01639625.2015.1012409>

- Liao, D.-L., Hong, C.-J., Shih, H.-L., & Tsai, S.-J. (2004). Possible Association between Serotonin Transporter Promoter Region Polymorphism and Extremely Violent Crime in Chinese Males. *Neuropsychobiology*, 50(4), 284–287. <https://doi.org/10.1159/000080953>
- Lim, A., Brewer, N., & Young, R. L. (2023). Revisiting the Relationship between Cybercrime, Autistic Traits, and Autism. *Journal of Autism and Developmental Disorders*, 53(4), 1319–1330. <https://doi.org/10.1007/s10803-021-05207-1>
- Lim, H.-W. (2021). A Study on Countermeasures Against Cyber Infringement Considering CPTED. *International Journal of Advanced Culture Technology*, 9(2), 106–117. <https://doi.org/10.17703/IJACT.2021.9.2.106>
- Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact.*, 26(5), 32:1-32:28. <https://doi.org/10.1145/3336141>
- Livingston, G., Cooper, C., Woods, J., Milne, A., & Katona, C. (2008). Successful ageing in adversity: The LASER–AD longitudinal study. *Journal of Neurology, Neurosurgery & Psychiatry*, 79(6), 641–645. <https://doi.org/10.1136/jnnp.2007.126706>
- Livingston, J. A., Testa, M., & VanZile-Tamsen, C. (2007). The Reciprocal Relationship Between Sexual Victimization and Sexual Assertiveness. *Violence Against Women*, 13(3), 298–313. <https://doi.org/10.1177/1077801206297339>
- Longobardi, C., Settanni, M., Fabris, M. A., & Marengo, D. (2020). Follow or be followed: Exploring the links between Instagram popularity, social media addiction, cyber victimization, and subjective happiness in Italian adolescents. *Children and Youth Services Review*, 113, 104955. <https://doi.org/10.1016/j.childyouth.2020.104955>
- Low, J. (2019). A Pragmatic Definition of the Concept of Theoretical Saturation. *Sociological Focus*, 52(2), 131–139. <https://doi.org/10.1080/00380237.2018.1544514>

- LSB. (2024, October 3). *CRM Code for Authorised Push Payment fraud winds down having more-than trebled reimbursement rates, slashed average losses, and slowed scam growth*. Lending Standards Board. <https://www.lendingstandardsboard.org.uk/crm-code-for-authorised-push-payment-fraud-winds-down-having-more-than-trebled-reimbursement-rates-slashed-average-losses-and-slowed-scam-growth/>
- Lusthaus, J., Bruce, M., & Phair, N. (2020). Mapping the Geography of Cybercrime: A Review of Indices of Digital Offending by Country. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 448–453. <https://doi.org/10.1109/EuroSPW51379.2020.00066>
- Macdonald, S. J., Donovan, C., & Clayton, J. (2023). ‘I may be left with no choice but to end my torment’: Disability and intersectionalities of hate crime. *Disability & Society*, 38(1), 127–147. <https://doi.org/10.1080/09687599.2021.1928480>
- Maden, M., Cunliffe, A., McMahon, N., Booth, A., Carey, G. M., Paisley, S., Dickson, R., & Gabbay, M. (2017). Use of programme theory to understand the differential effects of interventions across socio-economic groups in systematic reviews—A systematic methodology review. *Systematic Reviews*, 6(1), 266. <https://doi.org/10.1186/s13643-017-0638-9>
- Madon, S., Willard, J., Gyll, M., & Scherr, K. C. (2011). Self-Fulfilling Prophecies: Mechanisms, Power, and Links to Social Problems. *Social and Personality Psychology Compass*, 5(8), 578–590. <https://doi.org/10.1111/j.1751-9004.2011.00375.x>
- Maier, S. F., & Seligman, M. E. (1976). Learned helplessness: Theory and evidence. *Journal of Experimental Psychology: General*, 105(1), 3–46. <https://doi.org/10.1037/0096-3445.105.1.3>
- Makila Beni, R., Mbale Kasunzi Mbaherya, L., Muhau, J.-A., & Ilunga Wa Kuwita, G. (2024). An Empirical Study on Insider Threats Towards Crime Prevention Through Environmental Design (CPTED): A Student Case Study. In N. Naik, P. Jenkins, S. Prajapat, & P. Grace (Eds.), *Contributions Presented at The International Conference on Computing, Communication,*

- Cybersecurity and AI, July 3–4, 2024, London, UK* (pp. 447–463). Springer Nature Switzerland.
https://doi.org/10.1007/978-3-031-74443-3_27
- Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample Size in Qualitative Interview Studies: Guided by Information Power. *Qualitative Health Research*, 26(13), 1753–1760.
<https://doi.org/10.1177/1049732315617444>
- Mariano, J., Marques, S., Ramos, M. R., Gerardo, F., Cunha, C. L. da, Girenko, A., Alexandersson, J., Stree, B., Lamanna, M., Lorenzatto, M., Mikkelsen, L. P., Bundgård-Jørgensen, U., Rêgo, S., & de Vries, H. (2021). Too old for technology? Stereotype threat and technology use by older adults. *Behaviour & Information Technology*, 41(7), 1503–1514.
<https://doi.org/10.1080/0144929X.2021.1882577>
- Martin, A. (2024, August 5). *Replacement for Action Fraud, UK's cybercrime reporting service, delayed again until 2025*. The Record. <https://therecord.media/uk-action-fraud-replacement-delayed-2025>
- Mason, C. (2019, May 28). *Victim of a money transfer scam? You now have new rights with most banks*. MoneySavingExpert.Com.
<https://www.moneysavingexpert.com/news/2019/05/more-protection-for-money-transfer-scam-victims-from-today/>
- Mawby, R. I. (2017). Defensible Space. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. <https://doi.org/10.1093/acrefore/9780190264079.013.6>
- McGuire, M., & Dowling, S. (2013, October). *Cyber crime: A review of the evidence. Chapter 1: Cyber-dependent crimes*. Home Office.
<https://assets.publishing.service.gov.uk/media/5a7c83c1ed915d48c241043f/horr75-chap1.pdf>
- McLeod, S. (2024, January 25). *Erikson's Stages of Development*.
<https://www.simplypsychology.org/erik-erikson.html>

- Meijwaard, S. C., Kikkert, M., Mooij, L. D. de, Lommerse, N. M., Peen, J., Schoevers, R. A., Van, R., Wildt, W. de, Bockting, C. L. H., & Dekker, J. J. M. (2015). Risk of Criminal Victimization in Outpatients with Common Mental Health Disorders. *PLOS ONE*, 10(7), e0128508. <https://doi.org/10.1371/journal.pone.0128508>
- Melk, A., Tegtbur, U., Hilfiker-Kleiner, D., Eberhard, J., Saretzki, G., Eulert, C., Kerling, A., Nelius, A.-K., Hömme, M., Strunk, D., Berliner, D., Röntgen, P., Kück, M., Bauersachs, J., Hilfiker, A., Haverich, A., Bara, C., & Stiesch, M. (2014). Improvement of biological age by physical activity. *International Journal of Cardiology*, 176(3), 1187–1189. <https://doi.org/10.1016/j.ijcard.2014.07.236>
- Merryweather, L. (2021, October 18). *Scams impact on victims' wellbeing amounts to £9.3bn - Which? News*. Which? <https://www.which.co.uk/news/article/scams-impact-on-victims-costs-9-3-billion-a-year-a5mNq6i9316q>
- Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., Zych, I., & Paek, H.-J. (2024). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. *International Journal of Offender Therapy and Comparative Criminology*, 68(5), 449–467. <https://doi.org/10.1177/0306624X20981041>
- Miller, L. M. S., Callegari, R. A., Abah, T., & Fann, H. (2024). Digital Literacy Training for Low-Income Older Adults Through Undergraduate Community-Engaged Learning: Single-Group Pretest-Posttest Study. *JMIR Aging*, 7, e51675. <https://doi.org/10.2196/51675>
- Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth Internet Victimization in a Broader Victimization Context. *Journal of Adolescent Health*, 48(2), 128–134. <https://doi.org/10.1016/j.jadohealth.2010.06.009>
- Morrow, J. (2022, August 16). Co-Creation, Participatory Research, Co-Design, or Participatory Design... Which is it? *Medium*. <https://medium.com/@Josh.Morrow.1/co-creation-participatory-research-co-design-or-participatory-design-which-is-it-fa14a7f542c1>

- MPS. (2021). *Cyber Protect: How we can help your business*. Metropolitan Police.
<https://www.met.police.uk/advice/advice-and-information/wsi/watch-schemes-initiatives/cyber-protect/cyber-protect-how-we-can-help-your-business/>
- Nam, S., Han, S. H., & Gilligan, M. (2019). Internet Use and Preventive Health Behaviors Among Couples in Later Life: Evidence from the Health and Retirement Study. *The Gerontologist*, 59(1), 69–77. <https://doi.org/10.1093/geront/gny044>
- Näsi, M., Danielsson, P., & Kaakinen, M. (2023). Cybercrime Victimization and Polyvictimisation in Finland—Prevalence and Risk Factors. *European Journal on Criminal Policy and Research*, 29(2), 283–301. <https://doi.org/10.1007/s10610-021-09497-0>
- Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), 203–210. <https://doi.org/10.1080/14043858.2015.1046640>
- National Cybersecurity Alliance. (2025, January 17). *What is Multifactor Authentication (MFA) and Why Should You Use It?* <https://www.staysafeonline.org/articles/multi-factor-authentication>
- National Institute on Aging. (2019, April 23). *Social isolation, loneliness in older people pose health risks*. National Institute on Aging. <https://www.nia.nih.gov/news/social-isolation-loneliness-older-people-pose-health-risks>
- National Institute on Aging. (2021, July 8). *What Is Alzheimer’s Disease?* National Institute on Aging. <https://www.nia.nih.gov/health/alzheimers-and-dementia/what-alzheimers-disease>
- National Institute on Aging. (2024, July 11). *Loneliness and Social Isolation—Tips for Staying Connected*. National Institute on Aging. <https://www.nia.nih.gov/health/loneliness-and-social-isolation/loneliness-and-social-isolation-tips-staying-connected>
- NCA. (2020). *National Cyber Crime Unit: “A day in the life.”*
<https://www.nationalcrimeagency.gov.uk/careers/a-day-in-the-life/a-day-in-the-life-national-cyber-crime-unit-operations>

NCSC. (2021, November 26). *Phishing: Spot and report scam emails, texts, websites and calls*.

National Cyber Security Centre. <https://www.ncsc.gov.uk/collection/phishing-scams>

NCSC. (2023). *Cyber security regulations and directors duties in the UK*.

<https://www.ncsc.gov.uk/collection/board-toolkit/cyber-security-regulation-and-directors-duties-in-the-uk>

Ndubueze, P. N., Igbo, E. U. M., & Okoye, U. O. (2013). Cyber Crime Victimization among Internet

active Nigerians: An Analysis of SocioDemographic Correlates. *International Journal of*

Criminal Justice Sciences, 8(2). [https://ijcjs.com/menu-](https://ijcjs.com/menu-script/index.php/ijcjs/article/view/136)

[script/index.php/ijcjs/article/view/136](https://ijcjs.com/menu-script/index.php/ijcjs/article/view/136)

Newman, O. (1997). *Creating Defensible Space*. DIANE Publishing.

Ng, R., Chow, T. Y. J., & Yang, W. (2022). The Impact of Aging Policy on Societal Age Stereotypes and

Ageism. *The Gerontologist*, 62(4), 598–606. <https://doi.org/10.1093/geront/gnab151>

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and

Situational level factors. *International Journal of Cyber Criminology*, 5.

NHS. (2024, June). *Primary Care Dementia Data, June 2024*. NHS England Digital.

<https://digital.nhs.uk/data-and-information/publications/statistical/primary-care-dementia-data/june-2024>

NIHR. (2024, May). *Briefing notes for researchers—Public involvement in NHS, health and social care*

research. [https://www.nihr.ac.uk/briefing-notes-researchers-public-involvement-nhs-](https://www.nihr.ac.uk/briefing-notes-researchers-public-involvement-nhs-health-and-social-care-research)

[health-and-social-care-research](https://www.nihr.ac.uk/briefing-notes-researchers-public-involvement-nhs-health-and-social-care-research)

NIMH. (2024, December). *Traumatic Events and Post-Traumatic Stress Disorder (PTSD)*. National

Institute of Mental Health (NIMH). [https://www.nimh.nih.gov/health/topics/post-traumatic-](https://www.nimh.nih.gov/health/topics/post-traumatic-stress-disorder-ptsd)

[stress-disorder-ptsd](https://www.nimh.nih.gov/health/topics/post-traumatic-stress-disorder-ptsd)

NIMH. (2025, January). *Autism Spectrum Disorder—National Institute of Mental Health (NIMH)*.

<https://www.nimh.nih.gov/health/topics/autism-spectrum-disorders-asd>

- Norris, F. H., & Kaniasty, K. (1994). Psychological distress following criminal victimization in the general population: Cross-sectional, longitudinal, and prospective analyses. *Journal of Consulting and Clinical Psychology*, 62(1), 111–123. <https://doi.org/10.1037/0022-006X.62.1.111>
- North Yorkshire Police. (2024). *What happens when you report to Action Fraud?*
<https://www.supportingvictims.org/wp-content/uploads/2021/08/Action-Fraud-guidance-for-victims.pdf>
- Notten, N., & Nikken, P. (2016). Boys and girls taking risks online: A gendered perspective on social context and adolescents' risky online behavior. *New Media & Society*, 18(6), 966–988.
<https://doi.org/10.1177/1461444814552379>
- Ofcom. (2024, July 30). *Gen Z swerves traditional broadcast TV as less than half tune in weekly*. Ofcom. <https://www.ofcom.org.uk/media-use-and-attitudes/media-habits-adults/gen-z-swerves-traditional-broadcast-tv-as-less-than-half-tune-in-weekly/>
- Oliveira, D., Muradoglu, M., Soliman, D. W. A., & Ebner, T. L. N. (2017). *Dissecting Spear Phishing Emails for Older vs Young Adults: On the Interplay of Weapons of Influence and Life Domains in Predicting Susceptibility to Phishing*. 13.
- O'Malley, R. L., Holt, K., & Holt, T. J. (2022). An Exploration of the Involuntary Celibate (Incel) Subculture Online. *Journal of Interpersonal Violence*, 37(7–8), NP4981–NP5008.
<https://doi.org/10.1177/0886260520959625>
- Online Safety Act 2023 (2023). <https://www.legislation.gov.uk/ukpga/2023/50>
- ONS. (2019, March 4). *Exploring the UK's digital divide*. Office for National Statistics.
<https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04>
- ONS. (2021, April 6). *Internet users, UK*. Office for National Statistics.
<https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2020>

- ONS. (2022, November 29). *Language, England and Wales*. Office for National Statistics.
<https://www.ons.gov.uk/peoplepopulationandcommunity/culturalidentity/language/bulletins/languageenglandandwales/census2021#english-language-proficiency>
- ONS. (2023a). *Profile of the older population living in England and Wales in 2021 and changes since 2011—Office for National Statistics*.
<https://www.ons.gov.uk/peoplepopulationandcommunity/birthsdeathsandmarriages/ageing/articles/profileoftheolderpopulationlivinginenglandandwalesin2021andchangessince2011/2023-04-03>
- ONS. (2023b, February 8). *Disability by age, sex and deprivation, England and Wales*. Office for National Statistics.
<https://www.ons.gov.uk/peoplepopulationandcommunity/healthandsocialcare/disability/articles/disabilitybyagesexanddeprivationenglandandwales/census2021>
- ONS. (2024, March 6). *Crime in England and Wales, victim characteristics*. Office for National Statistics.
<https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/crimeinenglandandwalesvictimcharacteristics/yearendingmarch2023#main-points>
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533–544. <https://doi.org/10.1007/s10488-013-0528-y>
- Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, 120, 106745. <https://doi.org/10.1016/j.chb.2021.106745>
- Pandian, T., & Maraimalai, N. (2024). Understanding cybercrime's impact on women's physical and psychological well-being. *African Journal of Reproductive Health*, 28(5), Article 5. <https://ajrh.info/index.php/ajrh/article/view/4505>

- Payne, B. K. (2020). Criminals Work from Home during Pandemics Too: A Public Health Approach to Respond to Fraud and Crimes against those 50 and above. *American Journal of Criminal Justice*, 45(4), 563–577. <https://doi.org/10.1007/s12103-020-09532-6>
- Payne, B., May, D. C., & Hadzhidimova, L. (2019). America's most wanted criminals: Comparing cybercriminals and traditional criminals. *Criminal Justice Studies*, 32(1), 1–15. <https://doi.org/10.1080/1478601X.2018.1532420>
- Peacock, A. (2022, June 3). *The difference between co-design and participatory design*. Medium. <https://uxdesign.cc/difference-between-co-design-participatory-design-df4376666816>
- Pel-Littel, R. E., Schuurmans, M. J., Emmelot-Vonk, M. H., & Verhaar, H. J. J. (2009). Frailty: Defining and measuring of a concept. *The Journal of Nutrition, Health and Aging*, 13(4), 390–394. <https://doi.org/10.1007/s12603-009-0051-8>
- Pemberton, A., & Mulder, E. (2023). Bringing injustice back in: Secondary victimization as epistemic injustice. *Criminology & Criminal Justice*, 17488958231181345. <https://doi.org/10.1177/17488958231181345>
- Petersen, R. C., & Negash, S. (2008). Mild Cognitive Impairment: An Overview. *CNS Spectrums*, 13(1), 45–53. <https://doi.org/10.1017/S1092852900016151>
- Peterson, C., & Seligman, M. E. P. (1983). Learned Helplessness and Victimization. *Journal of Social Issues*, 39(2), 103–116. <https://doi.org/10.1111/j.1540-4560.1983.tb00143.x>
- Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2(2), Article 2. <https://doi.org/10.3390/forensicsci2020028>
- Pires, S. F., Guerette, R. T., & Stubbert, C. H. (2014). The Crime Triangle of Kidnapping for Ransom Incidents in Colombia, South America: A 'Litmus' Test for Situational Crime Prevention. *The British Journal of Criminology*, 54(5), 784–808. <https://doi.org/10.1093/bjc/azu044>

- Piroozfar, P., Farr, E. R. P., Aboagye-Nimo, E., & Osei-Berchie, J. (2019). Crime prevention in urban spaces through environmental design: A critical UK perspective. *Cities*, 95, 102411.
<https://doi.org/10.1016/j.cities.2019.102411>
- Poppleton, S., Lymperopoulou, K., & Molina, J. (2021, October 13). *Who suffers fraud? Understanding the fraud victim landscape*. Victims Commissioner.
- Porter, L. E., & Graycar, A. (2016). Hotspots of corruption: Applying a problem-oriented policing approach to preventing corruption in the public sector. *Security Journal*, 29(3), 423–441.
<https://doi.org/10.1057/sj.2013.38>
- Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and Routine Activity Theories Revisited: The Importance of “Risk” to the Study of Victimization. *Victims & Offenders*, 11(3), 335–354.
<https://doi.org/10.1080/15564886.2015.1057351>
- Prihadi, K. D., Hui, Y. L., Chua, M. J., & Chang, C. K. W. (2019). Cyber-victimization and perceived depression: Serial mediation of self-esteem and learned-helplessness. *International Journal of Evaluation and Research in Education (IJERE)*, 8(4), Article 4.
<https://doi.org/10.11591/ijere.v8i4.20266>
- Prince, M., Knapp, M., Guerchet, M., McCrone, P., Prina, M., Comas-Herrera, A., Wittenberg, R., Adelaja, B., Hu, B., King, D., Rehill, A., & Salimkuma, D. (2014). *Dementia UK: Update*. Alzheimer’s Society.
https://www.alzheimers.org.uk/sites/default/files/migrate/downloads/dementia_uk_update.pdf
- Prowse, D. (2014, November 25). Being the Green Cross Man beats being Darth Vader any day. *The Guardian*. <https://www.theguardian.com/commentisfree/2014/nov/25/david-prowse-green-cross-man-darth-vader-children-road-safety>
- Pryor, M., & McLaughlin, A. C. (2018). Developing Video or Multimedia Instructions for Older Adults. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 62(1), 1739–1743. <https://doi.org/10.1177/1541931218621394>

- PSR. (2023). *Policy statement: Fighting authorised push payment scams: Final decision*.
- Rabiner, D. J., O’Keeffe, J., & Brown, D. (2006). Financial Exploitation of Older Persons: Challenges and Opportunities to Identify, Prevent, and Address It in the United States. *Journal of Aging & Social Policy*, 18(2), 47–68. https://doi.org/10.1300/J031v18n02_04
- Raval, D. (2021). Who is Victimized by Fraud? Evidence from Consumer Protection Cases. *Journal of Consumer Policy*, 44(1), 43–72. <https://doi.org/10.1007/s10603-020-09466-w>
- Reckert, K. (2024, December 20). *UK-Erhebung: Ältere verlieren mehr durch Cybercrime | Sicherheits-Berater*. <https://www.sicherheits-berater.de/>. <https://www.sicherheits-berater.de/nachrichten/uk-erhebung-aeltere-verlieren-mehr-durch-cybercrime/>
- Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science*, 7(1), 5. <https://doi.org/10.1186/s40163-018-0079-3>
- Refundee. (2024). *What banks are signed up to the Contingent Reimbursement Model Code?* <https://www.refundee.com/blog/what-banks-are-signed-up-to-the-contingent-reimbursement-model-code>
- Restivo, E., & Lanier, M. M. (2015). Measuring the Contextual Effects and Mitigating Factors of Labeling Theory. *Justice Quarterly*, 32(1), 116–141. <https://doi.org/10.1080/07418825.2012.756115>
- Reyes, M. C. (2024, May 5). Beyond Mindfulness: A Critical Perspective in the Face of Domestic Violence. *Medium*. <https://medium.com/@chuforg/beyond-mindfulness-a-critical-perspective-in-the-face-of-domestic-violence-2e297a9ac574>
- Reyns, B. W., & Englebrecht, C. M. (2010). The stalking victim’s decision to contact the police: A test of Gottfredson and Gottfredson’s theory of criminal justice decision making. *Journal of Criminal Justice*, 38(5), 998–1005. <https://doi.org/10.1016/j.jcrimjus.2010.07.001>
- Rhoads, J. (2023). Psychological Effects of Cybercrime on Minorities: Short-Term and Long-Term Impacts. *Journal of Empirical Social Science Studies*, 7(1), Article 1.

- Ritchie, J., & Spencer, L. (1994). Qualitative data analysis for applied policy research. In *Analyzing Qualitative Data*. Routledge.
- ROCU. (2024a). *Cyber Crime*. Regional Organised Crime Unit Network.
<https://www.rocu.police.uk/capabilities/cyber-crime/>
- ROCU. (2024b). *Our National Network*. Regional Organised Crime Unit Network.
<https://www.rocu.police.uk/our-national-network/>
- Roller, M. R. (2020, February 16). Focus Groups: Heterogeneity vs. Homogeneity. *Research Design Review*. <https://researchdesignreview.com/2020/02/16/focus-groups-heterogeneity-vs-homogeneity/>
- Rosales, A., Fernández-Ardèvol, M., & Svensson, J. (2023). *Digital Ageism: How it Operates and Approaches to Tackling it* (1st ed.). Routledge. <https://doi.org/10.4324/9781003323686>
- Rudnicka, E., Napierała, P., Podfigurna, A., Męczekalski, B., Smolarczyk, R., & Grymowicz, M. (2020). The World Health Organization (WHO) approach to healthy ageing. *Maturitas*, 139, 6–11.
<https://doi.org/10.1016/j.maturitas.2020.05.018>
- Rupert, D. J., Poehlman, J. A., Hayes, J. J., Ray, S. E., & Moultrie, R. R. (2017). Virtual Versus In-Person Focus Groups: Comparison of Costs, Recruitment, and Participant Logistics. *Journal of Medical Internet Research*, 19(3), e6980. <https://doi.org/10.2196/jmir.6980>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. *Sensors*, 23(15), Article 15. <https://doi.org/10.3390/s23156666>
- Salisbury, H., & Upson, A. (2004). *Ethnicity, victimisation and worry about crime: Findings from the 2001/2 and 2002/3 British Crime Surveys* (Research Findings No. 237). Home Office.
- Satchell, J., Craston, T., Drennan, V. M., Billings, J., & Serfaty, M. (2023a). Psychological Distress and Interventions for Older Victims of Crime: A Systematic Review. *Trauma, Violence, & Abuse*, 24(5), 3493–3512. <https://doi.org/10.1177/15248380221130354>

- Satchell, J., Craston, T., Drennan, V. M., Billings, J., & Serfaty, M. (2023b). Psychological Distress and Interventions for Older Victims of Crime: A Systematic Review. *Trauma, Violence & Abuse*, 24(5), 3493–3512. <https://doi.org/10.1177/15248380221130354>
- SCCJR. (2016, February). Causes of Crime. *Theories and Causes of Crime*.
<https://www.sccjr.ac.uk/wp-content/uploads/2016/02/SCCJR-Causes-of-Crime.pdf>
- Schiks, J. A. M., van de Weijer, S. G. A., & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, 126, 106985.
<https://doi.org/10.1016/j.chb.2021.106985>
- Schultz, K., Cattaneo, L. B., Sabina, C., Brunner, L., Jackson, S., & Serrata, J. V. (2016). Key roles of community connectedness in healing from trauma. *Psychology of Violence*, 6(1), 42–48.
<https://doi.org/10.1037/vio0000025>
- SCIE. (2015). *Types and indicators of abuse* (No. At a glance 69). Social Care Institute for Excellence.
- SDSAF. (2023, October 25). *Research Project into Cyber Crime*.
<https://www.sdsaf.org.uk/news/research-project-into-cyber-crime/>
- Sentencing Council. (2025). *General Guideline – Vulnerable Victim*.
<https://www.sentencingcouncil.org.uk/droppable/item/general-guideline-vulnerable-victim/>
- Serfaty, M., Aspden, T., Satchell, J., Kessel, A., Laycock, G., Brewin, C. R., Buszewicz, M., O’Keeffe, A., Hunter, R., Leavey, G., Cuming-Higgs, J., Drennan, V., Riveros, M., Andrew, D., & Blanchard, M. (2020). The clinical and cost-effectiveness of a Victim Improvement Package (VIP) for the reduction of chronic symptoms of depression or anxiety in older victims of common crime (the VIP trial): Study protocol for a randomised controlled trial. *Trials*, 21(1), 333.
<https://doi.org/10.1186/s13063-020-4211-9>
- Shah, M. H., Jones, P., & Choudrie, J. (2019). Cybercrimes prevention: Promising organisational practices. *Information Technology & People*, 32(5), 1125–1129.
<https://doi.org/10.1108/ITP-10-2019-564>

- Shaw, C. R., & McKay, H. D. (1942). *Juvenile delinquency and urban areas* (pp. xxxii, 451). University of Chicago Press.
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373–382. <https://doi.org/10.1145/1753326.1753383>
- Shichor, D. (2014). Lombroso, Cesare. In *The Encyclopedia of Criminology and Criminal Justice* (pp. 1–5). John Wiley & Sons, Ltd. <https://doi.org/10.1002/9781118517383.wbeccj152>
- Sixsmith, A., Horst, B. R., Simeonov, D., & Mihailidis, A. (2022). Older People’s Use of Digital Technology During the COVID-19 Pandemic. *Bulletin of Science, Technology & Society*, 42(1–2), 19–24. <https://doi.org/10.1177/02704676221094731>
- Skivington, K., Matthews, L., Simpson, S. A., Craig, P., Baird, J., Blazeby, J. M., Boyd, K. A., Craig, N., French, D. P., McIntosh, E., Petticrew, M., Rycroft-Malone, J., White, M., & Moore, L. (2021). A new framework for developing and evaluating complex interventions: Update of Medical Research Council guidance. *BMJ*, 374, n2061. <https://doi.org/10.1136/bmj.n2061>
- Snyder, J. A., & Golladay, K. A. (2024). It Happened Again: Differences Between Single and Repeat/Poly-Victimization Among Financial Fraud Victims. *Journal of White Collar and Corporate Crime*, 5(1), 46–57. <https://doi.org/10.1177/2631309X231195801>
- Social Mobility Commission. (2023, September 12). *Level of wealth*. https://social-mobility.data.gov.uk/mobility_outcomes/wealth/level_of_wealth/latest
- Soliman, S., & Beaman, J. (2014). One Piece of the Puzzle-Financial Exploitation and Elder Abuse. In R. M. Factora (Ed.), *Aging and Money: Reducing Risk of Financial Exploitation and Protecting Financial Resources* (pp. 19–30). Springer. https://doi.org/10.1007/978-1-4939-1320-6_2
- Stancu, A. L. (2021). SUBCULTURAL THEORIES OF DELINQUENCY AND CRIME. *Journal of Law and Administrative Sciences*, 16. <https://jolas.ro/wp-content/uploads/2021/12/jolas16a11.pdf>

- Stapleton, N. (2023). *BBC One—Scam Interceptors—Five scams to watch out for right now*. BBC.
<https://www.bbc.co.uk/programmes/articles/3M1LPtdbXrWFyqTyyNrCzT9/five-scams-to-watch-out-for-right-now>
- Steen, M., Manshot, M., & De Koning, N. (2011). Benefits of Co-design in Service Design Projects. *International Journal of Design*, 5(2), 53–60.
- Stouffer, C. (2023, July 18). *What is encryption? How it works + types of encryption*. Norton.
<https://us.norton.com/blog/privacy/what-is-encryption>
- Stryker, C., & Kavlakoglu, E. (2024, August 9). *What Is Artificial Intelligence (AI)? | IBM*. What Is Artificial Intelligence (AI)? <https://www.ibm.com/topics/artificial-intelligence>
- Surkalim, D. L., Luo, M., Eres, R., Gebel, K., Buskirk, J. van, Bauman, A., & Ding, D. (2022). The prevalence of loneliness across 113 countries: Systematic review and meta-analysis. *BMJ*, 376, e067068. <https://doi.org/10.1136/bmj-2021-067068>
- Suzuki, A., Sidebottom, A., Wortley, R., & Shimada, T. (2024). Repeat victimisation and the crime drop: Evidence from Japan. *Crime Prevention and Community Safety*, 26(1), 1–15.
<https://doi.org/10.1057/s41300-023-00196-y>
- Taber-Doughty, T., Shurr, J., Brewer, J., & Kubik, S. (2010). Standard care and telecare services: Comparing the effectiveness of two service systems with consumers with intellectual disabilities. *Journal of Intellectual Disability Research*, 54(9), 843–859.
<https://doi.org/10.1111/j.1365-2788.2010.01314.x>
- Taherdoost, H. (2022). How to Conduct an Effective Interview; A Guide to Interview Design in Research Study Authors. *International Journal of Academic Research in Management (IJARM)*, 11(1), 39–51.
- Tarling, R., & Morris, K. (2010). Reporting Crime to the Police. *The British Journal of Criminology*, 50(3), 474–490. <https://doi.org/10.1093/bjc/azq011>

- Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2016). The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave? *Justice Quarterly*, 33(5), 890–911.
<https://doi.org/10.1080/07418825.2014.994658>
- Tennant, F. (2025, January). *Mandatory recompense: New UK rules to tackle APP fraud*. Financier Worldwide. <https://www.financierworldwide.com/mandatory-recompense-new-uk-rules-to-tackle-app-fraud>
- Tharshini, N. (2024). Mate crime victimization against individuals with intellectual disability. *Advances in Mental Health and Intellectual Disabilities*, 19(1), 23–35.
<https://doi.org/10.1108/AMHID-06-2024-0019>
- The Chicago School. (2021, July 2). *What is Positivism in Criminology?* | *The Chicago School*. Insight Digital Magazine. <https://www.thechicagoschool.edu/insight/psychology/what-is-positivism-in-criminology/>
- Thompson, K. (2016, August 20). *The Labelling Theory of Crime*.
<https://revisesociology.com/2016/08/20/labelling-theory-crime-deviance/>
- Thompson, R. W., Arnkoff, D. B., & Glass, C. R. (2011). Conceptualizing Mindfulness and Acceptance as Components of Psychological Resilience to Trauma. *Trauma, Violence, & Abuse*, 12(4), 220–235. <https://doi.org/10.1177/1524838011416375>
- Tilley, N., & Sidebottom, A. (2014). Situational Crime Prevention. In *Encyclopedia of Criminology and Criminal Justice* (pp. 4864–4874). Springer, New York, NY. https://doi.org/10.1007/978-1-4614-5690-2_549
- Tilley, N., Tseloni, A., & Farrell, G. (2011). Income Disparities of Burglary Risk: Security Availability during the Crime Drop. *The British Journal of Criminology*, 51(2), 296–313.
<https://doi.org/10.1093/bjc/azr010>
- Toshchakova, V. A., Bakhtiari, Y., Kulikov, A. V., Gusev, S. I., Trofimova, M. V., Fedorenko, O. Yu., Mikhailitskaya, E. V., Popova, N. K., Bokhan, N. A., Hovens, J. E., Loonen, A. J. M., Wilffert, B., & Ivanova, S. A. (2018). Association of Polymorphisms of Serotonin Transporter (5HTTLPR)

- and 5-HT2C Receptor Genes with Criminal Behavior in Russian Criminal Offenders. *Neuropsychobiology*, 75(4), 200–210. <https://doi.org/10.1159/000487484>
- Treleaven, P., Barnett, J., Brown, D., Bud, A., Fenoglio, E., Kerrigan, C., Koshiyama, A., Sfeir-Tait, S., & Schoernig, M. (2023). *The Future of Cybercrime: AI and Emerging Technologies Are Creating a Cybercrime Tsunami* (SSRN Scholarly Paper No. 4507244). <https://doi.org/10.2139/ssrn.4507244>
- Tripathi, K., Robertson, S., & Cooper, C. (2019). A brief report on older people's experience of cybercrime victimization in Mumbai, India. *Journal of Elder Abuse & Neglect*, 31(4–5), 437–447. <https://doi.org/10.1080/08946566.2019.1674231>
- Tseloni, A., Thompson, R., Grove, L., Tilley, N., & Farrell, G. (2017). The effectiveness of burglary security devices. *Security Journal*, 30(2), 646–664. <https://doi.org/10.1057/sj.2014.30>
- UK Finance. (2023). *Over £55 Million Of Fraud Prevented In 2022 By Rapid Response Scheme*. UK Finance. <https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps55-million-fraud-prevented-in-2022-rapid-response-scheme>
- UK Parliament. (2022, October 18). *Justice response inadequate to meet scale of fraud epidemic*. <https://committees.parliament.uk/committee/102/justice-committee/news/173618/justice-response-inadequate-to-meet-scale-of-fraud-epidemic/>
- van de Weijer, S. G. A., & Leukfeldt, E. R. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407–412. <https://doi.org/10.1089/cyber.2017.0028>
- van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 16(4), 486–508. <https://doi.org/10.1177/1477370818773610>
- van Deursen, A. J., & Helsper, E. J. (2015). A nuanced understanding of Internet use and non-use among the elderly. *European Journal of Communication*, 30(2), 171–187. <https://doi.org/10.1177/0267323115578059>

- Van Volkom, M., Stapley, J. C., & Amaturio, V. (2014). Revisiting the Digital Divide: Generational Differences in Technology Use in Everyday Life. *North American Journal of Psychology*, 16(3), 557–574.
- Vidal-Pineiro, D., Wang, Y., Krogsrud, S. K., Amlien, I. K., Baaré, W. F., Bartres-Faz, D., Bertram, L., Brandmaier, A. M., Drevon, C. A., Düzel, S., Ebmeier, K., Henson, R. N., Junqué, C., Kievit, R. A., Kühn, S., Leonardsen, E., Lindenberger, U., Madsen, K. S., Magnussen, F., ... Fjell, A. (2021). Individual variations in ‘brain age’ relate to early-life factors more than to longitudinal brain change. *eLife*, 10, e69995. <https://doi.org/10.7554/eLife.69995>
- VISION. (2023, November). *Written evidence from The Violence, Health and Society (VISION consortium)*. UK Parliament. <https://committees.parliament.uk/writtenevidence/126111/pdf/>
- Von Kempkens, V. (2024, December 20). *Ältere leiden am stärksten unter Cybercrime*. ICTkommunikation. <https://ictk.ch/inhalt/%C3%A4ltere-leiden-am-st%C3%A4rksten-unter-cybercrime>
- Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
- Wall*, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime1. *International Review of Law, Computers & Technology*, 22(1–2), 45–63. <https://doi.org/10.1080/13600860801924907>
- Wallhed Finn, S., Mejlidal, A., Baskaran, R., & Nielsen, A. S. (2023). Effects of media campaign videos on stigma and attitudes towards treatment seeking for alcohol use disorder: A randomized controlled study. *BMC Public Health*, 23(1), 1919. <https://doi.org/10.1186/s12889-023-16811-4>
- Ward, D. A., Stafford, M. C., & Gray, L. N. (2006). Rational Choice, Deterrence, and Theoretical Integration. *Journal of Applied Social Psychology*, 36(3), 571–585. <https://doi.org/10.1111/j.0021-9029.2006.00061.x>

- Warwick, E., & Lees, L. (2022). Osmosis across defensible space: Observations and lessons from dérives in London during COVID-19. *Urban Geography*, 43(6), 810–820.
<https://doi.org/10.1080/02723638.2022.2039435>
- Watts, S. J., & Wright, L. E. (2021). Military combat, mental health, and crime: A preliminary test of a general strain theory model. *Criminal Justice Studies*, 34(2), 202–214.
<https://doi.org/10.1080/1478601X.2020.1860035>
- Waugh, E. (2024, December 13). *What Is Smishing?* Experian. <https://www.experian.com/blogs/ask-experian/what-is-smishing/>
- Weiss, K. G. (2010). Too Ashamed to Report: Deconstructing the Shame of Sexual Victimization. *Feminist Criminology*, 5(3), 286–310. <https://doi.org/10.1177/1557085110376343>
- West Mercia Police. (2021). *Police bank branch response scheme prevents nearly a million pounds of fraud in West Mercia in first half of 2021*. <https://www.westmercia.police.uk/news/west-mercia/news/2021/september/police-bank-branch-response-scheme-prevents-nearly-a-million-pounds-of-fraud-in-west-mercia-in-first-half-of-2021/>
- Weulen Kranenbarg, M., Ruiter, S., van Gelder, J.-L., & Bernasco, W. (2018). Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison. *Journal of Developmental and Life-Course Criminology*, 4(3), 343–364. <https://doi.org/10.1007/s40865-018-0087-8>
- White, A. M. (2001). I am because we are: Combined race and gender political consciousness among african american women and men anti-rape activists. *Women's Studies International Forum*, 24(1), 11–24. [https://doi.org/10.1016/S0277-5395\(00\)00167-9](https://doi.org/10.1016/S0277-5395(00)00167-9)
- Whitford, T. (2018). Cyber Defense for IMGs and NGOs Using Crime Prevention Through Environmental Design. In H. Prunckun (Ed.), *Cyber Weaponry: Issues and Implications of Digital Arms* (pp. 47–58). Springer International Publishing. https://doi.org/10.1007/978-3-319-74107-9_4

- Whitty, M. T. (2018). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105–109.
<https://doi.org/10.1089/cyber.2016.0729>
- Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. <https://doi.org/10.1108/JFC-10-2017-0095>
- WHO. (2023a, March 15). *Dementia*. World Health Organisation. <https://www.who.int/news-room/fact-sheets/detail/dementia>
- WHO. (2023b, October 20). *Mental health of older adults*. World Health Organisation.
<https://www.who.int/news-room/fact-sheets/detail/mental-health-of-older-adults>
- WHO. (2024, October 1). *Ageing and health*. <https://www.who.int/news-room/fact-sheets/detail/ageing-and-health>
- Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through Situational Crime Prevention. *Commun. ACM*, 52(9), 133–137.
<https://doi.org/10.1145/1562164.1562198>
- Wilson, R. S., Sytsma, J., Barnes, L. L., & Boyle, P. A. (2016). Anosognosia in Dementia. *Current Neurology and Neuroscience Reports*, 16(9), 77. <https://doi.org/10.1007/s11910-016-0684-z>
- Woodyatt, C. R., Finneran, C. A., & Stephenson, R. (2016). In-Person Versus Online Focus Group Discussions: A Comparative Analysis of Data Quality. *Qualitative Health Research*, 26(6), 741–749. <https://doi.org/10.1177/1049732316631510>
- Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. *Sage Open*, 7(2), 2158244017710292. <https://doi.org/10.1177/2158244017710292>
- Wortley, R., Sidebottom, A., Tilley, N., & Laycock, G. (2018). What is crime science? In R. Wortley, A. Sidebottom, N. Tilley, & G. Laycock (Eds.), *Routledge Handbook of Crime Science* (1st ed., pp. 1–30). Routledge. <https://doi.org/10.4324/9780203431405-1>

- Wrigley, A., & Dawson, A. (2016). Vulnerability and Marginalized Populations. In D. H. Barrett, L. W. Ortmann, A. Dawson, C. Saenz, A. Reis, & G. Bolan (Eds.), *Public Health Ethics: Cases Spanning the Globe*. Springer. <http://www.ncbi.nlm.nih.gov/books/NBK435787/>
- Wu, Y.-H., Damnéé, S., Kerhervé, H., Ware, C., & Rigaud, A.-S. (2015). Bridging the digital divide in older adults: A study from an initiative to inform older adults about new technologies. *Clinical Interventions in Aging*, 10, 193–201. <https://doi.org/10.2147/CIA.S72399>
- Wutich, A., Beresford, M., & Bernard, H. R. (2024). Sample Sizes for 10 Types of Qualitative Data Analysis: An Integrative Review, Empirical Guidance, and Next Steps. *International Journal of Qualitative Methods*, 23, 16094069241296206. <https://doi.org/10.1177/16094069241296206>
- Xu, X., Xu, T., Wei, J., & Chen, T. (2024). Gut microbiota: An ideal biomarker and intervention strategy for aging. *Microbiome Research Reports*, 3. <https://www.oaepublish.com/articles/mrr.2023.68>
- Xue, Q.-L. (2011). The Frailty Syndrome: Definition and Natural History. *Clinics in Geriatric Medicine*, 27(1), 1. <https://doi.org/10.1016/j.cger.2010.08.009>
- Yar, M. (2005). The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407–427. <https://doi.org/10.1177/147737080556056>
- Yu, L., Mottola, G., Barnes, L. L., Han, S. D., Wilson, R. S., Bennett, D. A., & Boyle, P. A. (2021). Correlates of Susceptibility to Scams in Community-Dwelling Older Black Adults. *Gerontology*, 67(6), 729–739. <https://doi.org/10.1159/000515326>
- Yucedal, B. (2010). *VICTIMIZATION IN CYBERSPACE: AN APPLICATION OF ROUTINE ACTIVITY AND LIFESTYLE EXPOSURE THEORIES* [Kent State University]. https://etd.ohiolink.edu/acprod/odb_etd/etd/r/1501/10?clear=10&p10_accession_num=ke nt1279290984

- Zaykowski, H., Allain, E. C., & Campagna, L. M. (2019). Examining the Paradox of Crime Reporting: Are Disadvantaged Victims More Likely to Report to the Police? *Law & Society Review*, 53(4), 1305–1340. <https://doi.org/10.1111/lasr.12440>
- Zhang, C., Miao, X., Wang, B., Thomas, R. J., Ribeiro, A. H., Brant, L. C. C., Ribeiro, A. L. P., & Lin, H. (2023). Association of lifestyle with deep learning predicted electrocardiographic age. *Frontiers in Cardiovascular Medicine*, 10. <https://doi.org/10.3389/fcvm.2023.1160091>

Appendices

Appendix 1: Study 1 participant information sheet (friends and family)

Title of Study: A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Name and Contact Details of Principal Investigator:

Kartikeya Tripathi, Department of Security and Crime Science, University College London

Benjamin Havers, Department of Security and Crime Science, University College London



Introduction

I would like to invite you to take part in my research on cybercrime against older adults. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

Please read the following information carefully and feel free to ask any questions. Once you have all of the information you need, please take your time to decide whether or not you would like to participate in this research.

What is the purpose of this part of the study?

The aim is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions and support providers (including friends and family members), in order to gain an understanding of the barriers to reporting and areas for improvement in current reporting mechanisms.

Why have I been invited to take part in the study?

You have been invited because you are friend or family member of an older person who has been a victim of cybercrime or attempted cybercrime.

Do I have to take part?

No, you do not have to take part; this interview is entirely voluntary. There will be no negative outcomes if you choose not to take part in this research. You may withdraw at any point. You can choose not to answer any question I ask if you would prefer not to.

What would happen if I agreed to take part?

I will arrange an interview at a mutually convenient time. This will be in person, or via Microsoft Teams. I will first ask you to state whether you give your consent, in accordance with the attached form. I will then ask you a series of questions about your experiences of cybercrime victimisation.

With your permission I will record the interview, but please note that audio recordings made during this research will be used only for analysis and for illustration in project reports. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings, except for a UCL-approved transcription service.

Virtual interviews will take place using Microsoft Teams. Participants should indicate whether they would like recordings and the interview to be with their camera on, that is video and audio, or switched off, audio only. In person interviews will be recorded on the MS Voice Recorder App.

If participants do not wish to be recorded at all, they will be unable to participate.

Recordings will be deleted as soon as the transcripts have been transcribed and transcriptions checked against original recordings. This will happen no later than 6 months after the date of interview. In the meantime, recordings will be stored in a password protected file in a UCL drive.

What are the advantages and disadvantages of taking part?

Participants will be offered a love2shop voucher of £30 in return for their participation in the study. The research will contribute to a PhD thesis that is developing an intervention to protect older people from cybercrime. Participants will be able to receive a research summary document following the conclusion of the study.

Is the research confidential?

All information collected about you during the course of the study would be kept strictly confidential. Personal data will be handled in accordance with the Data Protection Act 2018 and UK GDPR. Research data will be retained securely and in line with University College London data management policies. No individual will be identifiable in any publications arising from the research; anything you say will be anonymous.

What will happen to the results of the study?

Depending on its quality and success, the study may be academically published. The findings will be used to inform the development of an intervention to protect older people from cybercrime

What if a problem arises?

If any issues arise as a result of your participation in the research and you would like to discuss this, then please contact me at [REDACTED] It is advised that in the first instance you raise any concerns with myse . However, should you feel your complaint has not been handled satisfactorily then you may contact the Chair of the UCL Research Ethics Committee at: ethics@ucl.ac.uk.

Research team:

Principal Investigator: Dr Kartikeya Tripathi; [REDACTED]

&

Ben Havers; [REDACTED]

Local Data Protection Privacy Notice

The controller for this project will be University College London (UCL). The UCL Data Protection Officer provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk

This 'local' privacy notice sets out the information that applies to this particular study. Further information on how UCL uses participant information can be found in our 'general' privacy notice:

For participants in research studies, see <https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice>

The information that is required to be provided to participants under data protection legislation (GDPR and DPA 2018) is provided across both the 'local' and 'general' privacy notices.

The lawful basis that will be used to process your personal data is: 'public task' and 'research purposes' will be the lawful basis for processing special category data.

Your personal data will be processed so long as it is required for the research project. If we are able to anonymise or pseudonymise the personal data you provide we will undertake this and will endeavour to minimise the processing of personal data wherever possible.

If you are concerned about how your personal data is being processed, or if you would like to contact us about your rights, please contact UCL in the first instance at data-protection@ucl.ac.uk

Thank you for reading this information sheet and for considering taking part in this research study.

Appendix 2: Study 2 participant information sheet (professionals)

Title of Study: A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Name and Contact Details of Principal Investigator:

Kartikeya Tripathi, Department of Security and Crime Science, University College London



Benjamin Havers, Department of Security and Crime Science, University College London



Introduction

I would like to invite you to take part in my research on cybercrime against older adults. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

Please read the following information carefully and feel free to ask any questions. Once you have all of the information you need, please take your time to decide whether or not you would like to participate in this research.

What is the purpose of this part of the study?

The aim is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions and support providers (including friends and family members), in order to gain an understanding of the barriers to reporting and areas for improvement in current reporting mechanisms.

Why have I been invited to take part in the study?

You have been invited because you are an employee of the Police, Action Fraud, or a financial institution, or you provide support to one or more older adults as an employee of an organisation that specialises in supporting older adults.

Do I have to take part?

No, you do not have to take part; this interview is entirely voluntary. There will be no negative outcomes if you choose not to take part in this research. You may withdraw at any point. You can choose not to answer any question I ask if you would prefer not to.

What would happen if I agreed to take part?

I will arrange an interview at a mutually convenient time. This will be in person or via Microsoft Teams. I will first ask you to state whether you give your consent, in accordance with the attached form. I will then ask you a series of questions about your experiences of cybercrime victimisation.

With your permission I will audio-record the interview, but please note that audio recordings made during this research will be used only for analysis and for illustration in project reports. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings, except for a UCL-approved transcription service.

Virtual interviews will take place using Microsoft Teams. Participants should indicate whether they would like recordings and the interview to be with their camera on, that is video and audio, or switched off, audio only. In person interviews will be recorded on the MS Voice Recorder App.

If participants do not wish to be recorded at all, they will be unable to participate.

Recordings will be deleted as soon as the transcripts have been transcribed and transcriptions checked against original recordings. This will happen no later than 6 months after the date of interview. In the meantime, recordings will be stored in a password protected file in a UCL drive.

What are the advantages and disadvantages of taking part?

Participants will be offered a love2shop voucher of £30 in return for their participation in the study. The research will contribute to a PhD thesis that is developing an intervention to protect older people from cybercrime. Participants will be able to receive a research summary document following the conclusion of the study.

Is the research confidential?

All information collected about you during the course of the study would be kept strictly confidential. Personal data will be handled in accordance with the Data Protection Act 2018 and UK GDPR. Research data will be retained securely and in line with University College London data management policies. No individual will be identifiable in any publications arising from the research; anything you say will be anonymous.

What will happen to the results of the study?

Depending on its quality and success, the study may be academically published. The findings will be used to inform the development of an intervention to protect older people from cybercrime

What if a problem arises?

If any issues arise as a result of your participation in the research and you would like to discuss this, then please contact me at [REDACTED]. It is advised that in the first instance you raise any concerns with myself. However, should you feel your complaint has not been handled satisfactorily then you may contact the Chair of the UCL Research Ethics Committee at: ethics@ucl.ac.uk.

Research team:

Principal Investigator: Dr Kartikeya Tripathi; [REDACTED]

&

Ben Havers; [REDACTED]

Local Data Protection Privacy Notice

The controller for this project will be University College London (UCL). The UCL Data Protection Officer provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk

This 'local' privacy notice sets out the information that applies to this particular study. Further information on how UCL uses participant information can be found in our 'general' privacy notice:

For participants in research studies, see <https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice>

The information that is required to be provided to participants under data protection legislation (GDPR and DPA 2018) is provided across both the 'local' and 'general' privacy notices.

The lawful basis that will be used to process your personal data is: 'public task' and 'research purposes' will be the lawful basis for processing special category data.

Your personal data will be processed so long as it is required for the research project. If we are able to anonymise or pseudonymise the personal data you provide we will undertake this and will endeavour to minimise the processing of personal data wherever possible.

If you are concerned about how your personal data is being processed, or if you would like to contact us about your rights, please contact UCL in the first instance at data-protection@ucl.ac.uk

Thank you for reading this information sheet and for considering taking part in this research study.

Appendix 3: Study 2 participant information sheet (older adults)

Title of Study: A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Name and Contact Details of Principal Investigator:

Kartikeya Tripathi, Department of Security and Crime Science, University College London



Benjamin Havers, Department of Security and Crime Science, University College London



Introduction

I would like to invite you to take part in my research on cybercrime against older adults. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

Please read the following information carefully and feel free to ask any questions. Once you have all of the information you need, please take your time to decide whether or not you would like to participate in this research.

What is the purpose of this part of the study?

The aim is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions and support providers (including friends and family members), in order to gain an understanding of the barriers to reporting and areas for improvement in current reporting mechanisms.

Why have I been invited to take part in the study?

You have been invited because you are an older adult who has been a victim of cybercrime or attempted cybercrime.

Do I have to take part?

No, you do not have to take part; this interview is entirely voluntary. There will be no negative outcomes if you choose not to take part in this research. You may withdraw at any point. You can choose not to answer any question I ask if you would prefer not to.

You may choose to end the interview at any time. The interviewer will not push you to answer questions to any degree if you are not willing to speak. If you do begin to feel distressed then the interview can be paused, postponed or ended. You may wish to have to-hand a friend, family member or care giver to speak to, either in person or over the phone, in the event that you do feel uncomfortable. If you feel that you would like to report any incidents to the police, you may do so by calling 999 in an emergency, 101 if it is not an emergency. You can also make an anonymous report to Crimestoppers at <https://crimestoppers-uk.org/> or 0800 555 111. If you require support as a victim you may contact Victim Support UK at <https://www.victimsupport.org.uk/> or 08 08 16 89 111. For general support, Age UK offer a free, confidential advice line on 0800 678 1602.

What would happen if I agreed to take part?

I will arrange an interview at a mutually convenient time. This will be in person or via Microsoft Teams. I will first ask you to state whether you give your consent, in accordance with the attached form. I will then ask you a series of questions about your experiences of cybercrime victimisation.

With your permission I will audio-record the interview, but please note that audio recordings made during this research will be used only for analysis and for illustration in project reports. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings, except for a UCL-approved transcription service.

Virtual interviews will take place using Microsoft Teams. Participants should indicate whether they would like recordings and the interview to be with their camera on, that is video and audio, or switched off, audio only. In person interviews will be recorded on the MS Voice Recorder App.

If participants do not wish to be recorded at all, they will be unable to participate.

Recordings will be deleted as soon as the transcripts have been transcribed and transcriptions checked against original recordings. This will happen no later than 6 months after the date of interview. In the meantime, recordings will be stored in a password protected file in a UCL drive.

What are the advantages and disadvantages of taking part?

Participants will be offered a love2shop voucher of £30 in return for their participation in the study. The research will contribute to a PhD thesis that is developing an intervention to protect older people from cybercrime. Participants will be able to receive a research summary document following the conclusion of the study.

Is the research confidential?

All information collected about you during the course of the study would be kept strictly confidential. Personal data will be handled in accordance with the Data Protection Act 2018 and

UK GDPR. Research data will be retained securely and in line with University College London data management policies. No individual will be identifiable in any publications arising from the research; anything you say will be anonymous.

What will happen to the results of the study?

Depending on its quality and success, the study may be academically published. The findings will be used to inform the development of an intervention to protect older people from cybercrime

What if a problem arises?

If any issues arise as a result of your participation in the research and you would like to discuss this, then please contact me at [REDACTED]. It is advised that in the first instance you raise any concerns with myself. However, should you feel your complaint has not been handled satisfactorily then you may contact the Chair of the UCL Research Ethics Committee at: ethics@ucl.ac.uk.

Research team:

Principal Investigator: Dr Kartikeya Tripathi; [REDACTED]

&

Ben Havers; [REDACTED]

Local Data Protection Privacy Notice

The controller for this project will be University College London (UCL). The UCL Data Protection Officer provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk

This 'local' privacy notice sets out the information that applies to this particular study. Further information on how UCL uses participant information can be found in our 'general' privacy notice:

For participants in research studies, see <https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice>

The information that is required to be provided to participants under data protection legislation (GDPR and DPA 2018) is provided across both the 'local' and 'general' privacy notices.

The lawful basis that will be used to process your personal data is: 'public task' and 'research purposes' will be the lawful basis for processing special category data.

Your personal data will be processed so long as it is required for the research project. If we are able to anonymise or pseudonymise the personal data you provide we will undertake this and will endeavour to minimise the processing of personal data wherever possible.

If you are concerned about how your personal data is being processed, or if you would like to contact us about your rights, please contact UCL in the first instance at data-protection@ucl.ac.uk

Thank you for reading this information sheet and for considering taking part in this research study.

Appendix 4: Study 2 topic guide (friends and family)

A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Introduction: Thank you for agreeing to take part in this interview. As you know I am a researcher from University College London. In order to make sure that I don't miss anything, I will record our conversation on a digital recorder and then it will be professionally transcribed. Once the interview has been transcribed, I will ensure that everything will be anonymous so you can't be identified.

(Serfaty et al., 2020)

Description of research:

The aim of our study is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions, and friends and family who provide support to older adults.

We to gain an understanding of the barriers to reporting, with a view to identifying relevant shortcomings and areas for improvement in current reporting mechanisms. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

We also want to learn about the role and perspective of their friends, family and professionals who provide support and assist in the reporting process.

We have invited you to this interview as an you are a friend or family member who has supported an older adult through their cybercrime victimisation.

Q1. Please could you tell me what you understand about cybercrime?

- What does it look like?
- How might you identify cybercrime?
- What types of cybercrime exist?

Q2. Please could you tell me how somebody might report a cybercrime?

- What channels are available to report cybercrime?
- When should you report cybercrime to your bank?
- When should you report cybercrime to the police?
- Are you familiar with Action Fraud?
- Who else might you report it to?

Q2. I appreciate it might be difficult to recall, but can you tell me about your experience of supporting somebody with cybercrime?

- What happened?
- Were you able to offer them support?
- In what way?
- Did you encourage them to report the cybercrime? How?
- What were the challenges involved?
- Looking back, is there anything that you think you should have done differently?

- Did you change the nature of the support you give as a result of your experience?

Q3. Is there anything else you would like to tell me about your experiences that we haven't discussed?

Thank you very much for your time.

If you have any additional comments please do feel free to email me.

Appendix 5: Study 2 topic guide (older adults)

A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Introduction: Thank you for agreeing to take part in this interview. As you know I am a researcher from University College London. In order to make sure that I don't miss anything, I will record our conversation on a digital recorder and then it will be professionally transcribed. Once the interview has been transcribed, I will ensure that everything will be anonymous so you can't be identified.

Description of research:

The aim of our study is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions, and friends and family who provide support to older adults.

We to gain an understanding of the barriers to reporting, with a view to identifying relevant shortcomings and areas for improvement in current reporting mechanisms. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

We also want to learn about the role and perspective of their friends, family and professionals who provide support and assist in the reporting process.

We have invited you to this interview as an you are an older adult who has been targeted by cybercrime.

Q1. Please could you tell me what you understand about cybercrime?

- What does it look like?
- How might you identify cybercrime?
- What types of cybercrime do you think exist?

Q2. Please could you tell me how somebody might report a cybercrime?

- What channels do you think are available to report cybercrime?
- When do you think you should report cybercrime to your bank?
- When should you report cybercrime to the police?
- Are you familiar with Action Fraud? What do they do?
- Who else might you report it to?

Q3. I appreciate it might be difficult to recall, but can you tell me about your experience of cybercrime?

- What device were you using?
- What happened?
- Was it a single incident? How long did it go on for?
- Did you know the offender?
- What happened as a result?
- How did you feel during the victimisation?
- How did you feel after the victimisation?

Q4. Did you speak to anyone about it?

- Who?
- How did you feel about reporting it?
- Who did you report it to?
- (If they didn't report it) Why didn't you report it?
- Did you experience any difficulties reporting or attempting to report?
- Did you receive any support with reporting the cybercrime?
- Looking back, is there help or advice you wish you had had?
- Did you change how you used the internet after what happened? How?

Q5. Is there anything else you would like to tell me about your experiences that we haven't discussed?

Thank you very much for your time.

If you have any additional comments please do feel free to email

Appendix 6: Study 2 topic guide (professionals)

A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Introduction: Thank you for agreeing to take part in this interview. As you know I am a researcher from University College London. In order to make sure that I don't miss anything, I will record our conversation on a digital recorder and then it will be transcribed. Once the interview has been transcribed, I will ensure that everything will be anonymous so you can't be identified.

Description of research:

The aim of our study is to canvass the opinions, feelings and experiences of cybercrime victims aged 60 and over, relevant stakeholders from Action Fraud, Police, Financial institutions, other organisations, and friends and family who provide support to older adults.

We want to gain an understanding of the barriers to reporting, with a view to identifying relevant shortcomings and areas for improvement in current reporting mechanisms. We will explore how people aged 60+ who experience cybercrime respond to it, including how they decide whether to report it and to change their online behaviour.

We also want to learn about the role and perspective of their friends, family and professionals who provide support and assist in the reporting process.

We have invited you to this interview as you are an employee of the Police, Action Fraud, or a financial institution, or you provide support to one or more older adults as an employee of an organisation that supports older adults and vulnerable people.

Q1. Please tell me how you / your organisation might get involved with an older person who has experienced cybercrime?

- How do older people approach you or how do you get in touch with older people who have been victimised?
- Can you describe to me if there is a formal or informal mechanism to get this information? How does it work? What channels are available to report cybercrime?
- Can you tell me about a time you have done this? What happened?
- What types of cybercrime against the elderly have you come across? What was the nature of the scam/attack?
- What is the profile of older adults who fall victim to cybercrime? What factors make them more vulnerable?

Q2. I am interested in how to support older people to avoid cybercrime victimisation. Do you have any ideas about what helps?

- What in your experience might support people to report cybercrime?
- How can varying levels of digital literacy and access be addressed?
- How do you incentivise reporting?
- In your experience are there any particular factors that make older people vulnerable to cybercrime?
- If yes, what can we do about them? For example, mitigation strategies.

Q3. Is there anything else you would like to tell me about your experiences that we haven't discussed?

Thank you very much for your time.

If you have any additional comments please do feel free to email me.

Appendix 7: Study 2 consent form

CONSENT FORM

Title of Study: A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

Name and Contact Details of Principal Investigator:

Kartikeya Tripathi, Department of Security and Crime Science, University College London



Benjamin Havers, Department of Security and Crime Science, University College London



Name and Contact Details of the UCL Data Protection team: data-protection@ucl.ac.uk

This study was approved by UCL Research Ethics Committee (Application number 25325/001)

Thank you for considering taking part in this research. The person organising the research must explain the project to you before you agree to take part. If you have any questions arising from the Participant Information Sheet or explanation already given to you, please ask the researcher before you decide whether to take part. You will be given a copy of this Consent Form to keep and refer to at any time.

Please provide your consent to the bullet points below verbally to the interviewer before the interview commences. Alternatively, please state if you *do not* consent to the below points.

- I have read and understood the Participant Information Sheet provided. I have been given a full explanation by the investigators of the nature, purpose, location and duration of the study, and of what I will be expected to do.
- I have been given the opportunity to ask questions on all aspects of the study and have understood the advice and information given.

- I agree to comply with the requirements of the study as outlined to me to the best of my abilities. I shall inform the investigators immediately if I have any concerns.
- I agree for my anonymised data to be used for this study.
- I agree for my anonymised data to be used for any future research that will have received all relevant legal, professional and ethical approvals.
- I give consent to the interview being audio recorded and transcribed. I agree for my audio recording to be sent to a transcription company for transcription purposes.
- I give consent to quotations being used in reports so long as they are reported anonymously such that no individual, department and/or organisation is identified or identifiable.
- I understand that all project data will be held for 2 years and that my personal data is held and processed in the strictest confidence, and in accordance with the UK Data Protection Act (2018).
- I understand that I am free to withdraw from the study at any time without needing to justify my decision.
- I understand that I have 7 days from the date that the interview took place to indicate to the research team that I would like my responses to be withdrawn from the study.
- I understand the potential risks of participating in this study and the support that will be available to me should I become distressed during the course of the research.
- I understand the direct/indirect benefits of participating in this study.
- I understand that the data will not be made available to any commercial organisations but is solely the responsibility of the researchers undertaking this study.
- I am aware of who I should contact if I wish to lodge a complaint.
- I confirm that I have read and understood the above and freely consent to participating in this study. I have been given adequate time to consider my participation.

Appendix 8: Study 2 participant demographic questionnaire (friends & family)

Support Provider Identification Number:

Date of Interview:

Participant Initials:

Researcher Initials:

Informed Consent

1. Has the participant given consent? ☐ No ☐ Yes
2. Date participant gave consent:

Inclusion/ Exclusion Criteria

Inclusion Criteria			
The following criteria MUST be answered YES for participant to be included in the study:		Yes	No
1	Adult		
2	Has experience of providing support to one or more older adults as a friend or family member in the last 12 months		
Exclusion Criteria			
The following criteria MUST be answered NO for participant to be included in the study		Yes	No
1	Unwilling to consent		
Confirmation of Eligibility			
Researcher's Name:	Signature:	Date:	

Demographic data

Please answer the following questions.

Age:

.....

Gender: ☐ Male ☒ Female ☐ Other ☐ Prefer not to say

Ethnicity:

☐ White ☐ Mixed/Multiple ethnic groups ☐ Asian/Asian British ☐
Black/African/Caribbean/Black British ☐ Other ethnic group ☐ Prefer not to say

Relation:

☐ Partner ☐ Sibling ☒ Son/Daughter ☐ Grandchild ☐
Friend/Neighbour ☐ Other

Age:

☐ 18-30
☐ 30-40
☐ 40-50
☐ 50-60
☐ 60-70
☐ 80-90
☐ 90 and over

Nature of support:

☐ Physical
☐ Computer/device related
☐ Administrative
☐ Other

Appendix 9: Study 2 participant demographic questionnaire – older adults

Older Adult Identification Number:

Date of Interview:

Participant Initials:

Researcher Initials:

Informed Consent

1. Has the participant given consent? ☐NO ☐Yes
2. Date participant gave consent:

Inclusion/ Exclusion Criteria

Inclusion Criteria					
The following criteria MUST be answered YES for participant to be included in the study:			Yes	No	
1	Aged 65 years or older				
2	Has been a victim of a cybercrime or an attempted cybercrime				
Exclusion Criteria					
The following criteria MUST be answered NO for participant to be included in the study			Yes	NO	
1	Lacking capacity and/or unwilling to consent				
Confirmation of Eligibility					
Researcher's Name:		Signature:	Date:		

Demographic data

Please answer the following questions.

Age:

Gender: ☐Male ☐Female ☐Other ☐Prefer not to say

Ethnicity:

☐ White ☐ Mixed/Multiple ethnic groups ☐ Asian/Asian British ☐
Black/African/Caribbean/Black British ☐ Other ethnic group ☐ Prefer not to say

What is the highest level of education you have completed?

☐ Primary school ☐ Secondary school up to 16 years ☐ Higher or secondary or further education (A-levels, BTEC, etc.) ☐ College or university ☐ Post-graduate degree
☐ Prefer not to say

Tenure:

☐ Rented Social ☐ Rented Private ☐ Own Home ☐ Other ☐ Prefer not to say

Living situation:

☐ Alone ☐ With Partner ☐ With family ☐ Other ☐ Supported Living ☐ Prefer not to say

Device used most for using the internet

☐ Phone ☐ Tablet ☐ Computer ☐ Other ☐ Prefer not to say

Hours spent on the internet per week

☐ 0-2 ☐ 2-4 ☐ 4-6 ☐ 6-8 ☐ 8+ ☐ Prefer not to say

Type of harm/loss as a result of cybercrime

☐ Financial minor ☐ Financial moderate ☐ Financial significant ☐ Emotional minor ☐ Emotional moderate ☐ Emotional significant ☐ Prefer not to say

☐ Money recovered

Appendix 10: Study 2 participant demographic questionnaire – professionals

Professional Identification Number:

Date of Interview:

Participant Initials:

Researcher Initials:

Informed Consent

1. Has the participant given consent? ☐NO ☐Yes

2. Date participant gave consent: 20/09/2023

3. Inclusion/ Exclusion Criteria

Inclusion Criteria				
The following criteria MUST be answered YES for participant to be included in the study:			Yes	No
1	Adult			
2	Works for the Police / Action Fraud / a financial institution / an organisation that provides support to older adults			
Exclusion Criteria				
The following criteria MUST be answered NO for participant to be included in the study			Yes	NO
1	Unwilling to consent			
Confirmation of Eligibility				
Researcher's Name:		Signature:	Date:	

Demographic data

Please answer the following questions:

Age:

.....

Gender: Male ☐ Female ☐ Other ☐ Prefer not to say

Ethnicity:

☐ White ☐ Mixed/Multiple ethnic groups ☐ Asian/Asian British ☐
Black/African/Caribbean/Black British ☐ Other ethnic group ☐ Prefer not to say

Organisation:


☐ Police ☐ Action Fraud ☐ Financial Institution ☐ Other care worker ☐ Assisted Living Worker

Role:

Years Experience in said role, or similar role

Appendix 11: Study 2 infographic (older adults)


Department of Security and Crime Science



Are you aged 60+ and in the UK?
Have you experienced a scam or fraud online in the past year?

We would like to hear from you!


- Participants will take part in a short, confidential interview, virtually or in-person
- You will be offered a £30 Love2shop voucher in exchange for your time

The aim of the study is to identify and address shortcomings in current cybercrime reporting mechanisms. If you're interested in hearing more, please contact Ben Havers at 

This project has received approval from the UCL Research Ethics Committee, ref 25325/001

Appendix 12: Study 2 infographic (family, friends and health and social care professionals)

Department of Security and Crime Science



Do you care for an over 60 in the UK?

Have you ever experienced a scam or fraud online in the past year?

We would like to hear from you!


Participants will take part in a short, confidential interview, virtually or in-person

✓ You will be offered a £30 Love2shop voucher in exchange for your time

The aim of the study is to identify and address shortcomings in current cybercrime reporting mechanisms. If you're interested in hearing more, please contact Ben Havers at [redacted]


This project has received approval from the UCL Research Ethics Committee, ref 25325/001

Department of Security and Crime Science

 **UCL**

Are you aged 60+?


Have you experienced a scam or fraud
online in the past year?



We would like to hear from you!

- ✓ Participants will take part in a short, confidential interview, either virtually or in-person
- ✓ You will be offered a £30 Love2shop voucher in exchange for your time

If you're interested in hearing more about this study,
please contact Ben Havers at



This project has received approval from the UCL Research Ethics Committee, ref 25325/001

Appendix 14: Study 2 ethics approval



26th July 2023

Dr Kartikeya Tripathi
Department of Security and Crime Science
UCL

Cc: Benjamin Havers, Postgraduate Research Student, UCL Department of Security and Crime Science

Dear Dr Tripathi

Notification of Ethics Approval with Provisos

Project ID/Title: 25325/001: A qualitative exploration of the barriers to reporting cybercrime among older adults in the UK

I am pleased to confirm in my capacity as Chair of the UCL Research Ethics Committee (REC) that your application has been ethically approved by the UCL REC until **26th July 2024.**

Ethical approval is subject to the following conditions:

Notification of Amendments to the Research

You must seek Chair's approval for proposed amendments (to include extensions to the duration of the project) to the research for which this approval has been given. Each research project is reviewed separately and if there are significant changes to the research protocol you should seek confirmation of continued ethical approval by completing an 'Amendment Approval Request Form'

<https://www.ucl.ac.uk/research-ethics/responsibilities-after-approval>

Adverse Event Reporting – Serious and Non-Serious

It is your responsibility to report to the Committee any unanticipated problems or adverse events involving risks to participants or others. The Ethics Committee should be notified of all serious adverse events via the Ethics Committee Administrator (ethics@ucl.ac.uk) immediately the incident occurs. Where the adverse incident is unexpected and serious, the Joint Chairs will decide whether the study should be terminated pending the opinion of an independent expert. For non-serious adverse events the Joint Chairs of the Ethics Committee should again be notified via the Ethics Committee Administrator within ten days of the incident occurring and provide a full written report that should include any amendments to the participant information sheet and study protocol. The Joint Chairs will confirm that the incident is non-serious and report to the Committee at the next meeting. The final view of the Committee will be communicated to you.


Final Report

At the end of the data collection element of your research we ask that you submit a very brief report (1-2 paragraphs will suffice) which includes in particular issues relating to the ethical implications of the research i.e. issues obtaining consent, participants withdrawing from the research, confidentiality, protection of participants from physical and mental harm etc.



Appendix 15: Study 3 social media publicity

Posts

**Ben Havers**

5 Jun · 🌐


Hi everyone,




I'm a PhD researcher at University College London. Official profile here:
<https://profiles.ucl.ac.uk/88942-benjamin-havers/about>


I'm currently recruiting over-60s to participate in a workshop about reporting online scams and cybercrime on Thursday 4th July at 2pm over Microsoft Teams. It will last up to 90 minutes and all participants will be offered £40 as a token of thanks for their time.

If you're interested in taking part, please send me an email at [redacted] and I will be happy to send over more information.

Thanks!

 profiles.ucl.ac.uk

  2 

 **Post insights** **VIEW**

Appendix 16: Study 3 consent form

CONSENT FORM

Co-designing interventions to tackle digital ageism around cybercrime victimisation

Name and Contact Details of Principal Investigator:

Kartikeya Tripathi, Department of Security and Crime Science, University College London



Benjamin Havers, Department of Security and Crime Science, University College London



Name and Contact Details of the UCL Data Protection Officer:

Alexandra Potts

This study was approved by UCL Research Ethics Committee (Application number 25325/002)

Thank you for considering taking part in this research. The person organising the research must explain the project to you before you agree to take part. If you have any questions arising from the Participant Information Sheet or explanation already given to you, please ask the researcher before you decide whether to take part. You will be given a copy of this Consent Form to keep and refer to at any time.

Please provide your consent to the bullet points below verbally to the workshop facilitator before the workshop commences. Alternatively, please state if you *do not* consent to the below points.

Points for consent	Y/N (please fill)
I have read and understood the Participant Information Sheet provided. I have been given a full explanation by the investigators of the nature, purpose, location and duration of the study, and of what I will be expected to do.	
I have been given the opportunity to ask questions on all aspects of the study and have understood the advice and information given.	

I agree to comply with the requirements of the study as outlined to me to the best of my abilities. I shall inform the investigators immediately if I have any concerns.	
I agree for my anonymised data to be used for this study.	
I agree for my anonymised data to be used for any future research that will have received all relevant legal, professional and ethical approvals.	
I give consent to the workshop being video recorded and transcribed.	
I give consent to quotations being used in reports so long as they are reported anonymously such that no individual, department and/or organisation is identified or identifiable. I understand that all project data will be held for 2 years and that my personal data is held and processed in the strictest confidence, and in accordance with the UK Data Protection Act (2018).	
I understand that I am free to withdraw from the study at any time without needing to justify my decision.	
I understand that I have 7 days from the date that the workshop took place to indicate to the research team that I would like my responses to be withdrawn from the study.	
I understand the direct/indirect benefits of participating in this study.	
I understand that the data will not be made available to any commercial organisations but is solely the responsibility of the researchers undertaking this study.	
I am aware of who I should contact if I wish to lodge a complaint.	
I confirm that I have read and understood the above and freely consent to participating in this study. I have been given adequate time to consider my participation.	
I confirm that I am happy to be recontacted after the workshop to comment on early findings derived from the workshop. There is no obligation to provide comment.	
I would like to receive a summary of the results and understand my contact details will be held for 3 months after the study has ended for this purpose.	
I confirm that I am happy for other workshop participants to receive my name, gender and occupation/role, but that these details should not be shared with any other party outside of the study.	

Name:

Date:

Appendix 17: Study 3 participant information sheet

Participant Information Sheet

Title of Study: Co-designing interventions to tackle digital ageism around cybercrime victimisation and reporting

UCL Research Ethics Committee Approval ref 25325/002

Name and Contact Details of Investigators:

Kartikeya Tripathi, Department of Security and Crime Science, University College London



Benjamin Havers, Department of Security and Crime Science, University College London



Introduction

I would like to invite you to take part in our research on cybercrime victimisation and reporting among older adults. Please read the following information carefully and feel free to ask any questions. Once you have all of the information you need, please take your time to decide whether or not you would like to participate in this research.

What is the purpose of this part of the study?

The aim of the study is to develop evidence-based strategies that can help support reporting by older victims of cybercrime. We are inviting you to participate in a small-group workshop lasting up to 90 minutes, over Microsoft Teams.

Why have I been invited to take part in the study?

You have been invited because you have expertise in this area, through your professional work or lived experience.

Do I have to take part?

No, you do not have to take part; participation is entirely voluntary. There will be no negative outcomes if you choose not to take part in this research. You may withdraw at any point. You can choose not to answer any question if you would prefer not to.

What would happen if I agreed to take part?

In advance of the workshop, you will be sent an evidence summary sheet and information about the event. During the workshop you will be invited to contribute to discussions about the evidence. There will be four to six participants in each workshop. I will record the workshop.

What are the advantages and disadvantages of taking part?

Participants will be offered £40 as a thank you for their time and trouble. The research will contribute to a PhD thesis on developing an intervention to protect older people from cybercrime. Participants will be able to receive a research summary document following the conclusion of the study.

Is the research confidential?

All information collected about you during the course of the study will be kept strictly confidential. Personal data will be handled in accordance with the Data Protection Act 2018 and UK GDPR. Research data will be retained securely and in line with University College London data management policies. No individual will be identifiable in any publications arising from the research; anything you say will be anonymous. Audio recordings made during this research will be used only for analysis and for illustration in project reports. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recordings.

What will happen to the results of the study?

The study will be published. The findings will be used to inform the development of an intervention to protect older people from cybercrime.

What if a problem arises?

If any issues arise as a result of your participation in the research and you would like to discuss this, then please contact me at [REDACTED]. It is advised that in the first instance you raise any concerns with one of the principal investigators. However, should you feel your complaint has not been handled satisfactorily then you may contact the Chair of the UCL Research Ethics Committee at: ethics@ucl.ac.uk.

Research team:

Principal Investigator: Dr Kartikeya Tripathi: [REDACTED]

Ben Havers: [REDACTED]

Local Data Protection Privacy Notice

The controller for this project will be University College London (UCL). The UCL Data Protection Officer provides oversight of UCL activities involving the processing of personal data, and can be contacted at data-protection@ucl.ac.uk

This 'local' privacy notice sets out the information that applies to this particular study. Further information on how UCL uses participant information can be found in our 'general' privacy notice:

For participants in research studies, see <https://www.ucl.ac.uk/legal-services/privacy/ucl-general><https://www.ucl.ac.uk/legal-services/privacy/ucl-general-research-participant-privacy-notice>

The information that is required to be provided to participants under data protection legislation (GDPR and DPA 2018) is provided across both the 'local' and 'general' privacy notices. The lawful basis that will be used to process your personal data is: 'public task'. Your personal data will be processed so long as it is required for the research project. If we are able to anonymise or pseudonymise the personal data you provide we will undertake this and will endeavour to minimise the processing of personal data wherever possible. If you are concerned about how your personal data is being processed, or if you would like to contact us about your rights, please contact UCL in the first instance at data-protection@ucl.ac.uk

Thank you for reading this information sheet and for considering taking part in this research study.

Appendix 18: Study 3 direct solicitation message

Dear (invitee name),

I would like to invite you to take part in an online workshop for a UCL research project about cybercrime reporting.

In the workshop, I will share my recent research findings about how older people experience and report cybercrime, and ask the group how we should use them to make a difference to how cybercrime victims are supported. We can offer a £40 shopping voucher as a token of thanks for your participation.

Please let me know if you would be interested to know more.

Best wishes,

Ben Havers

PhD Candidate

Dawes Centre for Future Crime

UCL Department of Security and Crime Science



25325/002

Appendix 19: Study 3 workshop agenda

Agenda: Co-producing interventions to tackle digital ageism in cybercrime victimisation (25325/002)

1. Welcome and introductions
2. Presentation:
 - Introduction to the project
 - Overview of evidence base that will inform intervention design
 - Introduction to the draft Theory of Change (ToC), study outcomes and goals
3. Proposing and developing intervention ideas
4. What needs to be in place for the outputs to be successful so that the outcomes occur?
5. Thanks and next steps.

Appendix 20: Study 3 framework matrix

Activity	Activity Component	Workshop			
		Health and social care professionals	Other professional stakeholders	Older adults 1	Older adults 2
Holding interactive cybersecurity sessions that bring older adults together	Creating an environment that allows older adults to feel comfortable about opening up	<i>This project has come at the same time as a course we are having to teach older people IT. I had 16 people, and we went through your briefing pack together. When I mentioned your research about scams, once we started talking about it, other people started opening up about scams that have happened to them. I think that maybe an intervention that would probably be pretty good would be if we did have these kinds of courses out there – IT courses for older people who would like to learn, and so that they can be with other people they can discuss it with together.</i>	<i>Over the last eight years of supporting fraud victims, both reactively and proactively when doing community engagement work, you will find a large number of people come up to you at the end of a session to say, “that did happen to me, but I haven’t reported it” for reason X, Y and Z. There were a lot of older adults there and there were questions about cybercrime and what they could do to safeguard themselves, and some of them did come up to me and said that they had been victims of cybercrime. Not very many had reported it. They didn’t know what to do. So I think there is an element of value in finding places where older people are more likely to socialise and congregate, and targeting an intervention there.</i>		
	Capitalising on the common desire to socialise and learn to impart cybercrime and reporting advice	<i>I had a really old lady, I think she’s late 80s, early 90s, but with very good advice that she started opening up about. She received a text message saying that her daughter dropped her mobile phone down the toilet, asking that she sends her some money. She actually got up out of her seat to come over to the flip chart that I had, to look at everything that I was writing down. Everyone seemed really interested in the topic of conversation as well, so maybe bring in IT courses and having those conversations might be less stigmatizing.</i>		<i>Many people belong to U3A [University of the Third Age], for example, [it] has 400,000 members nationwide divided into over a thousand separate branches. It might be a very good idea to see if you can get some talks. Either a set talk that’s given to local U3As, with trained speakers. And also the national organization does online talks – several a month – and that would be a very good way of reaching a number of people, although in all honesty it’ll probably be about attendance of about 200 people at each zoom event. But it’s [what is key] is trying to find the groupings of people I think. It’s probably the most economical way of getting out information.</i>	<i>The reason I’ve come into contact with this [study] is because I volunteer at a session where they have dozens of people who go there just for a social event.</i>

	Providing educational resources with universal messaging to aid session facilitators and for attendees to take home	<i>I think there is usually somebody that's a bit better at this stuff than others - and that's fairly resource neutral to have a team champion – and I suppose where this research could go would be to provide some resources for that champion, because you don't need very much, do you? You need the kind of basic advice that's sensible to give, and then with ways of onward referring, perhaps with recommendations that if it's an online onward referral, they might want a sort of trusted person to help them do that.</i>	<i>One of the issues that we constantly come across is that fraud campaigns have not been successful due to the large amount of differing information that people are getting. The messaging is complicated, so any type of leaflets or fridge magnets will have to tie in with any national campaign that there is, so that the messaging is straightforward and consistent.</i>	<i>I think the important thing moving forward is to actually have some material available that can be put out to different organizations. The trouble is that most advertising actually costs you money, whether it's putting it on a bus or advertising in a newspaper. It all costs money. But having some kind of central message, imagine an A4 flyer perhaps, or even an A5 flyer initially, that can be distributed to lots of different places, or reproduced. It's also about encouraging dialogues as well; having discussions. To have presentations there or just leaflets there – just some way of targeting the people who might be the victims and saying this is what's available to you [in terms of support and advice and reporting options]. I mean, even if it's not something that's immediately happening, it may be there for them in the future when they need it. It would have to be simple, it would just be, say, a saying if you think you have been a victim of this crime, these are the places you can go to. Leaflets, fridge magnets... whatever! Just a little trinket that has contact numbers on and things like that.</i>	
Engaging previous victims of cybercrime to offer support and advice in different contexts	Setting up peer support helplines for victimised or concerned older adults		<i>Something I was thinking about when you were going through your presentation – and I think it also links back to the importance of having people around you and to the previous point around making it easier to report through other means that aren't digital – is a helpline, but one that is run by other elderly people who previously may have also had experiences of victimisation. I think something similar has</i>		

			<p>been done in Canada, but I'd have to double check that, but it would be a helpline that could be integrated into Action Fraud services or the third sector possibly, where elderly people are able to ring up to discuss their victimisation. They can then be referred onto other reporting mechanisms if necessary, or they can just have a chat about their experiences and any support that they might need. I think it's also valuable for those that run the helpline that have previously had experiences of victimisation to also help them overcome the feelings of blame, and understanding that this can happen to anyone really. I think that last point is good because that would reinforce the idea that it's cybercrime is very common and so individuals shouldn't feel ashamed of being scammed in some way because there are other people out there who they're talking to who have exactly the same experience.</p>		
	<p>Inviting previous victims to be guest speakers at cybersecurity sessions for older adults</p>	<p>[There is] a group that I that I run, and I run two sessions exploring new technologies and learning new skills. We're having these conversations about scams and things like that.... 'What are you worried about? – Well, I'm worried about cybercrime and things like that.' So I think by having these conversations, it's been quite nice. I mean, I said that "you know what? I was scammed on eBay" and then that's how we started off. I found out what people know and what people don't know. One person, he was scammed for £1400 and so then he knew about Action Fraud. He phoned them, Action Fraud got in touch with eBay, and he got his money back.</p>	<p>We've gone to care homes... we've gone to town halls; anywhere that you can promote an event. And we have trialled that. So normally you do get people coming up afterwards, but when we've done a couple of sessions with victims, there was an even greater response because then you would get people in the audience who disclose that it had happened to them, but they hadn't reported it. So what we did trial as well was actually doing sessions with somebody who has been a victim. So now there's one thing isn't there from a professional like myself doing a full awareness session. If you've got someone next to me that they can really relate to – someone you know that looks like them - you know that has gone through a similar experience... that had a great initial buzz of people actually reporting. And once again, it's for people to know they don't necessarily have to report to the police. They can go to a charity like ourselves and still be supported. For whatever reason, people might not want to report to the police and that's fine. So they shouldn't think that, you know, is a barrier to them being supported generally.</p>		
<p>Engaging younger demographics in educational</p>	<p>Organising IT help schemes where younger people can</p>	<p>We did have a charity, shut down now, [that was] bringing people together in the community. So a younger</p>			

and supporting roles	volunteer to be matched with older adults in need of IT support	<p>person would go around and teach an older person how to use IT. I thought that it's a shame that's not happening anymore, but that would have been quite helpful. They've done lots of different things, but that was one of the things that they used to do. Having younger people go around to teach older people to use IT just so that it could bring younger communities and older communities together more.</p> <p>I do wonder whether a good piece of advice would be... because we have had a lot of people that have had a gutful of waiting on the phone being put on hold. I mean quite clearly the non-online reporting mechanisms cannot cope at the moment, and if somebody could find a trusted person to support them to use the online mechanisms. I just wonder whether that is [also] something that you could perhaps put in a video?</p>			
	Translating and interpreting of cybersecurity advice, cybercrime reporting processes and potentially malicious communications by younger people for older adults whose first language is not English				<p>There are whole communities where I live in South Manchester. There are large communities where English isn't spoken at home really. You know, children and grandchildren would be the main sources of communicating with the older people in those families. I've seen it with my elderly in-laws. Anything in way complicated would be dealt with through their children or grandchildren. When looking at how to get reporting done it's not just something about the older community. It's trying to tackle that next generation down, who are probably the people who are gonna often help the older community. Neighbours, the friends. The person at the church, or the synagogue, or the mosque, who might be the trusted person who they'll talk to.</p>
Communicating messages that normalise and decatastrophise victimisation	Emphasising victim faultlessness	<p>So, [it is about] almost normalising it... a shift from making it this really big, scary cybercrime, [where] terrible things are gonna happen, to 'this is something that's reality now a part of our everyday. This is how many people have been affected, but don't worry because there's this and this. And actually it's really common. It's not rare at all. You're not on your own. It doesn't mean you're going to lose all your money, you just have to do this to safeguard yourself.' So like the shift from making it big and scary because, with the Internet, it's everywhere now. It's so common, isn't it!</p>	<p>So firstly, on the 'you're not to blame' message, I think now we're getting a better understanding of the social grooming element, aren't we. So it's about coercion. So it's about, I think, always emphasising that message and [that] it's nothing to do with your intelligence. You know, you have been groomed, in effect, by the perpetrator. And in terms of where to go to for reporting. So Action Fraud as it stands is going through a rebirth. So when it is relaunched, as you know, the UK's reporting centre for fraud, how are people going to know about that? Obviously none of us know the answer to that at the moment, but how is that</p>		<p>So there's something about education. It's okay to do this. Don't feel ashamed that you've been sucked in by somebody; a team of sophisticated people. They're very often scam teams, aren't they? It can happen to so many people so easily. I think shame is reduced by having more tools and knowing what to do.</p> <p>I mean, I'm cynical. So you know I won't believe anything is true until I've done all the research to believe it is. But young people are being scammed too, so there's something about not the over sixties don't have to feel that they're in this group of being</p>

			<p>going to reach people? So I'll be watching that closely as well. It [Action Fraud] hasn't always been met with the most favourable response, shall we say, from its service users. So hopefully the feedback we'll get from people [regarding its replacement service] is that it's easier to speak to somebody [than with Action Fraud], that you are getting better two-way communication etcetera.</p>		<p>a bit dodgery and not quite being with it because it crosses all age ranges.</p> <p>The other thing we've had this year is three or four different scams via telephone. I think they're just random. And I think that lots of older people feel that they've done something stupid that causes them personally to be targeted, whereas in practice it's random. You know, [begins to impersonate offender] 'we've got a mobile number, we're gonna try it and we'll see if we can get... you know... [some details]', and so I think people think they are personally being targeted, which immediately makes you shameful and vulnerable, rather than, you know, [recognising that] it's a fishing rod that's gone out trying to hook somebody. And so I think that telling you that that's what a lot of scams are, that they're just fishing – it's just a fishing expedition. I think that is something that would make people feel more aware that things might be scams, but also help to reduce some of the shameful feelings.</p>
	<p>Maximising message impact through TV and radio</p>	<p>I mean, it might be out there, but if there was a short two minute video that was endorsed by action fraud and so forth and gave the security information that was needed, then it could be shown in all of these different places. It could potentially be about building skills – you can get your clear message out. You would need to approach it with some multi-language communication. If you found there were particular communities being targeted, then you could tackle that. Or if each Borough Council had a reporting centre, they know the demographic of their people. They would know if there's a particularly Big Punjabi speaking population [for example].</p>	<p>So I'm thinking the long lines of if you think you're a victim, this is the website. This is the e-mail address. This is the telephone number. So just a simple list of three or four different places to go.</p> <p>[What is important is] making people aware of how they can report and who they should be reporting to, so there's no mixed messages or, you know, uncertainty around that.</p>	<p>I must say, I think that the program on BBC at the moment the scam interceptors, to me, is very relevant. It opens your mind apart from anything else. I mean, I'm fortunate, I've never, ever had any approaches which have led to anything bad or anything. But really that sort of thing does open your mind. I really think it's a real eye opener.</p> <p>I hear often on radio 4 the consumer programs, they quite frequently highlight scams and cybercrime issues, and we get stories of victims and how they've managed in most cases to seek redress. So I think there's quite a bit of information if you know where to look for there. They make me nervous initially, but then when I hear how people have resolved them, as is usually the case, I find that encouraging.</p>	<p>I partly have visions of, you know, like a television ad. Really, the Green Cross Code man, when I was young, things that stick with you. But there are so many, I mean, people have such mixed views of reporting anything these days because of the reception they'll get. It's not worth the bother. Nobody cares. and I think it's raising the bar and saying, yes, there is care, and this is where you contact.</p> <p>I think that the Green Cross Code is quite, you know, simple and accessible too. I mean, older people tend to watch television and adverts on television still. So there's still mass communication methods that older people are more receptive to than say younger people. So I think it's things like that, I think, would be useful to use.</p>
	<p>Making the most of NHS and care service to reach those in need of support</p>		<p>It's always about how is that messaging going to cut through, isn't it? No doubt you would have come across this from your other working group with social care professionals, but it's about the people that are in old peoples' homes that may not be looking at, say, [victim</p>		<p>The other thing is, doctors' surgeries have huge notice boards targeting all age groups for things. So yeah, I just think the country needs to be swamped, young and old, with information about what to do [in the event of victimisation].</p>

			support charity] Victim Support's social media for fraud awareness warnings. So it's about working with different services, isn't it. Care providers, etcetera.		
Training stakeholders on communicating empathetically and recognising victimisation signs	Using more empathetic and less victim blaming language when speaking with potential victims of cybercrime		<p>You need to be really careful in the use of language all the time. Like when I talk to people, they often say, oh, I feel really stupid that I fell for this. I'll always then want to explain to them that if it was any other crime, you wouldn't talk about having fallen for it, and people don't seem to view cybercrime as much of a crime as they would say Burglary or being assaulted or whatever. I think probably a lot of professionals are trying to change the way they frame things in the words that they use. But it's so ingrained that, you know, you fall for a scam. But it's kind of just like what people say without even thinking about it.</p>	<p>In terms of these sorts of feelings of stupidity [experienced post victimisation], it comes back again to this training, or possibly it's not training, but attitude with the banks and the financial institutions. I was sending a large sum of money to a solicitor recently, and I called up [the bank], and the first thing they've done is ask 'where did you get the bank details from'. I said email, and they say 'oh well the emails could have been intercepted'. So they put this fear into you. There's this kind of tone, if you like. You get this sort of feeling of getting so fearful of making some sort of mistake which would lead you to being blamed for the fraud happening to you. And I understand that there has to be a balance, because obviously they're trying to protect you. I'm not quite sure what the answer is.</p>	<p>There is a sort of tertiary point here, I suppose there is something which crops up in my mind. I don't know if there's any stats on this. You know how many people report things that they think are a scam that turn out not to be. I think there's something here about how that's dealt with in terms of the people being made to feel stupid or embarrassed. It's the sort of 'cry wolf' thing, isn't it? If someone rings up, it's like, "Oh, no, don't be stupid". If the underlying attitude is, you know, a bit like when you get sent to Accident and Emergency by the doctor and the A and E people think "what are you doing here". That's the sense you get, you know. If that comes across on something which perhaps looks suspicious to you, but in fact not to be, could you potentially be dissuaded from raising [legitimate] issues?</p> <p>My wife got very concerned about some scam that was going on – I don't remember, but she was so concerned. She reported it, and within an hour a young policeman knocked the door, and he was offering comfort and guidance. And we thought, 'wow', you know, 'I didn't expect that'. Every day I read the police neighbourhood reports, and a lot of them are related to scams. I will admit to finding the comfort of having this young six foot two young man, very interested, empathetic, but above all, it was giving my wife the confidence to know that there were genuine people out there, and these scammers probably just one in a million. Most of the people in this world, especially the British, are very caring, that's my experience. And they would do all they can to help keep the peace. I've got long COVID. My mind's going. I'm old. I can't remember what the scam was, but my wife at the time was quite concerned, and not only for herself, but for our daughter and other people. She did tick a box, in this report – 'do you want some kind of intervention or response?' And the thing is, we got it. To my surprise, my delightful surprise.</p>

					<p><i>I had a similar very good experience like that with a burglary, actually, where the forensics guy suddenly turned up at my door because he'd heard the case on the [police] radio. If you feel vindicated and listened to, then that obviously to the average person is actually worth a lot. Or, you know, not only being listened to but the attitude when you're listened to – I think those two things couple together and are incredibly important in what we're talking about here.</i></p>
	<p>Upskilling stakeholders to provide sound advice and to recognise and act on signs of victimisation</p>	<p><i>Here, I do a 'lifestyle matters' programme. So we have these kinds of conversations and yeah, I must admit, we don't have the training on it really to talk about cybercrime. In fact, when it gets brought up, it's just a conversation that we end up having a discussion about amongst ourselves. So yeah, I we need to learn more.</i></p>	<p><i>One of the contributing factors [to victimisation] can be loneliness or loss of a spouse – going through a difficult period in their lives – and it's at that time when they're vulnerable that they need the support, but they don't seek it or don't know how to seek it. And the NHS has this huge, you know, network in place in order to do something about it, and to contribute to [tackling] it by identifying these individuals who are at risk or who are being victimised.</i></p>		

Appendix 21: Study 3 ethics approval



Student name: Benjamin Havers

Supervisor name: Kartikeya Tripathi

Project ID: 785

Title of proposed project: Co-designing interventions to tackle digital ageism around cybercrime victimisation

Upon review of the materials that you provided, the Department of Security and Crime Science Ethics Committee has decided to grant your project ethics approval under the low-risk category.

The approval is granted for the duration of the project mentioned in your application. If the project continues beyond this period, you will need to seek an extension or a fresh approval.

Should your project substantially change from what you have proposed, you will need to go through the ethics approval process again.

Signe



Dated: 09/05/2024

Dr Kartikeya Tripathi

Chair, Departmental Ethics Committee
Department of Security and Crime Science
University College London

Author contribution statement

The PhD title was proposed by the Dawes Centre for Future Crime at UCL, who funded me for three years. With the regular support, advice and assistance of my supervisory team consisting of Professor Claudia Cooper (QMUL) and Doctors Kartikeya Tripathi (UCL) and Alexandra Burton (QMUL) I conceived and conducted all the research within, and wrote this PhD thesis. Professor Sally McManus (City) and Dr Wendy Martin (Brunel) contributed to the writing of two of my research articles which are featured. Dr Aiden Sidebottom (UCL) acted as my upgrade examiner, during which he advised on the general direction of study.