Wiley
Health & Social Care in the Community
Volume 2024, Article ID 1314265, 10 pages
https://doi.org/10.1155/2024/1314265

WILEY

Research Article

Exploring the Factors Preventing Older Adults From Reporting Cybercrime and Seeking Help: A Qualitative, Semistructured Interview Study

Benjamin Havers,[1] **Kartikeya Tripathi**,[1] **Alexandra Burton**,[2] **Wendy Martin**,[3] **and Claudia Cooper**[4]

[1] *Dawes Centre for Future Crime, Department of Security and Crime Science, Faculty of Engineering, University College London, London, UK*
[2] *Department of Behavioural Science and Health, University College London, London, UK*
[3] *Department of Health Sciences, Brunel University London, Uxbridge, UK*
[4] *Centre for Psychiatry and Mental Health, Wolfson Institute of Population Health, Queen Mary University of London, London, UK*

Correspondence should be addressed to Benjamin Havers; benjamin.havers.20@ucl.ac.uk

Received 17 May 2024; Accepted 3 October 2024

Academic Editor: Tracy Collins

Background: Older adults under-report cybercrime, despite being more likely than younger people to experience repeat victimisation, financial loss and more severe emotional consequences. Considering vulnerabilities more common in old age, we sought to identify, and consider ways to address, barriers that older people experience when reporting cybercrime to statutory agencies with a role in reporting.
Methods: From community groups, police and victim support, and health and social care organisations, we purposively invited people aged 60+ who had experienced cybercrime ($n = 16$), their supporting family members ($n = 2$) and professional stakeholders ($n = 15$) to participate in semistructured in-person or virtual interviews and conducted a reflexive thematic analysis.
Results: Across 33 interviews, we identified four themes: (1) Shame and fear of repercussion; (2) Reporting unhelpful to emotional and financial recovery; (3) Lack of knowledge of scams and sources of support; and (4) Social support makes a difference.
Conclusions: Digital ageism, evidenced by structural barriers, stigma and disempowerment experienced by older adults deciding whether to report cybercrime, warrants attention from the FJN and authorities. Independent "advocates" such as health, social care and third sector professionals can support older victims of cybercrime to navigate such reporting challenges.

Keywords: cybercrime older reporting shame digital ageism

1. Introduction

The global cost of cybercrime is estimated at several trillions of pounds a year [1]. The UK (United Kingdom) has the highest density of cybercrime victims among developed nations, at 4371 per million internet users [2]. The growing number of older people with online access, expedited by the pandemic [3], has many positive benefits for society and individuals, but increases exposure of this demographic group to cybercriminals [4].

Older adults experience emotional harm [5] and psychological distress [6] as a result of fraud and cybercrime victimisation; those with greater health and social needs may be particularly vulnerable to these effects. In a recent analysis of data from the 2019–2020 Crime Survey for England and Wales, 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 [7]. 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 [8].

Cybercrime may be particularly likely to be under-reported (e.g., [9] in comparison with traditional crime). A study by Wall [10] suggested that victims may consider cybercrime less worthy of reporting than traditional crime because it is informational rather than physical. Though Graham et al. [11] acknowledge that internet users are now much more familiar with, and willing to report, online offences, they propose that victims' overall beliefs around the likelihood of arrest are significantly greater for traditional crime than for cybercrime. Correia [12] claims that victims may not see the benefit in reporting as they anticipate an ineffective response. Other proposed reasons behind cybercrime under-reporting include victim embarrassment [13, 14] and a lack of knowledge regarding what constitutes an offence, where and how to report it [15].

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. [16] 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.

Pervasive, ageist, victim blaming societal attitudes can discourage reporting 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) [17] collective term for the multiple agencies available for reporting cybercrime). Ageism can be defined as 'the complex, often negative construction of old age, which takes place at the individual and the societal levels' [18]. *Digital* ageism is 'the implicit or explicit discrimination of older adults based on how age is represented and experienced in relation to digital technologies' [19].

Rosales et al. [19] proposed 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* refers 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 [19]. There is presently no published research exploring digital ageism within fraud and cybercrime reporting mechanisms.

This is the first 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. [16] programme theory and Rosales et al. [19] interpersonal and corporate conceptual model of digital ageism, we aim to identify the barriers that older adults face when deciding whether to report cybercrime, and explore how they might be mitigated.

2. Materials and Methods

2.1. Participants and Procedures. UCL Research Ethics Committee, reference 25,325/001 approved the study. We 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. We publicised the study nationally on Facebook, Nextdoor, Twitter and LinkedIn, and through our existing networks with third sector organisations and health and care, and FJN professionals. We invited participants to tell others about the study.

We recruited: (1) People aged 60+ who reported experiencing cybercrime in the last five years, defined as online fraud or computer misuse. We included individuals who had engaged with malicious actor(s) or content over the internet. We did not include people who had received, but not engaged with phishing emails or other malicious content, or who lacked capacity to consent. Capacity to consent was determined by BH, who had undertaken Mental Capacity Act 2005 training, under the supervision of consultant old age psychiatrist CC. We only included people with capacity to consent to take part in the research, but did not explicitly exclude people with mild cognitive impairment. We 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 5 years. They could be, but were not necessarily the friends or family members of the people aged 60+ we interviewed. (3) Professional stakeholders, whose professional role included supporting, in a frontline or management role, older people experiencing cybercrime. We purposively recruited professionals from policing, bank, health and social care and third sector organisations. We recorded participants' sociodemographic characteristics and role characteristics for professional stakeholders.

Qualitative interviews followed semistructured topic guides (Appendices 1–3). We opted for semistructured 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. Semistructured interviews allow the researcher to guide the conversation through unexpected yet pertinent topics without significant restriction [20], respecting the fact that this is a sensitive topic. 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 or in-person, at the participant's preference, and lasted 30–60 min. Recognising that the topic might be difficult to talk about the interviewer 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 we 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, none of the older adults interviewed became visibly upset. Interviews were all conducted, recorded and transcribed by BH, a mixed-methods researcher with semistructured interview experience and a background in policing.

2.2. Analysis. We 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 [21]. Reflexivity in this study manifested as iterative examination, adaptation and refinement of themes, initially generated by BH, between our multidisciplinary team of authors. With backgrounds encompassing crime science and policing (KT, BH), 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 our findings in accordance with our respective areas of expertise. Subjectivity was approached with open dialogue in meetings, chaired by CC, and our themes and descriptions reflect a collaborative interpretation of the interview data drawn from interconnecting whilst distinct approaches. Braun and Clarke's [21] 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. [16] programme theory and Rosales et al. [19] 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. Phase 2 was *coding*; working through the dataset and applying labels to segments of text that appeared potentially relevant or meaningful. Phase 3 was *generating initial themes*, clustering codes into broader patterns and ideas. Phase 4 was *developing and reviewing themes*, whereby themes are reassessed and compared with other themes and against the entire dataset. Phase 5 was *refining, defining and naming themes*. The final phase, 6, was the *writing up*. We consulted WM at this stage, due to her expertise in digital ageism from a social gerontological perspective.

BH carried out the analysis; a sample of the interview transcripts was shared and discussed by CC, AB and KT, to consider emerging themes. We included quotations—selected for their illustrative efficacy—to emphasise key points. Whilst all interviews contributed directly or contextually to our resulting themes, not all were quoted.

3. Results

3.1. Sample Description. BH interviewed 33 participants between August 2023 and January 2024, 31 via video call and two in-person. Sixteen 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. We 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 ethnic group. Professional stakeholder participants worked in healthcare ($n = 5$), law enforcement ($n = 5$), third sector support organisations ($n = 2$), banking ($n = 2$) and IT ($n = 1$).

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. All used the internet for at least 6 hours a week, and four participants were online for over 30 h per week. Half ($n = 8$) had a postgraduate degree; others had 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 significant impacts. 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, three moderate, and seven reported significant impact.

3.2. Findings. We identified four themes, responding to our 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 makes a difference: 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.

We discuss these themes in depth below. Participant names have been replaced with pseudonyms.

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 this to family because it would have reflected negatively on him:

> Mike: *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: 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 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. 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.*

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.

> *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."*

Male community mental health nurse 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... 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 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.*

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 only 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. And I just didn't want to sort of put my head above the parapet with that one.*

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: *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 scammer] *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.*

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: 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.*

3.2.2. Reporting Perceived as Unhelpful to Emotional or Financial Recovery. Several older adults referenced the negative impact of the scam on their well-being, 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 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. (. . .) 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.*

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. 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 would not 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: *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, cybercriminals.

> 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. . . Every single week, we've nameless threat actors based abroad, which, you know, we've got no jurisdiction over.*

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: *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 we 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: *Quite frankly, the initial response, it was horrific. . . . 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.*

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.

> Rebekah: *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 victimisation.

> Kim: *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. You know, how can an intelligent person like me fall for that?*

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*: 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.*

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 us 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 MO increased the likelihood of victimisation, because the target is unable to identify or recognise threats:

> Blake: *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.* (...) *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.*

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: *I ordered something to come through the post and my mum received a* [fake] *DPD text related to a package being delivered, and so she thought that this was my package. 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: *Without being unkind to the people that we work with,* (...) *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 it.*

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 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 [technology] *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.*

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: [It is] *difficult for the bank employees because they're trying to protect people and their money from scams and things. (…) Older people feel patronised. I think older people probably get a bit irritated.*

3.2.4. Social Support Makes a Difference. A number of professional stakeholders, as well as older victims of cybercrime and family members, 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 could make:

Aaron: *The cyber security and scam awareness sessions are incredibly popular… I think because the media highlights scams quite a lot, especially over COVID as well. Like 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: *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, (…) 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.*

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. 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 themself. 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.

Alice: *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 Wesley suggested that victims could overcome their fear of negative perception by talking to someone neutral, who they trust not to make judgements.

Wesley: *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…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.*

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'.

A 69-year-old e-commerce 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.*

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. Discussion

4.1. Barriers to Reporting and the Value of Social Interaction. To our 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. Interviewees described how older adults feel shame, fear retribution and perceived negative sequelae of reporting often outweigh perceived benefits. Social interaction, including cybersecurity-focused local group "sessions" for older adults hosted by trusted authorities, was valued by both professional stakeholders and older adults as ways for raising awareness and tackle ageist stereotypes. 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. Limited awareness of cybercrime *modi victims operandi* and reporting channels were practical barriers to detection and disclosure.

4.2. Ageism and Under-Reporting. Of the risk factors leading to under-reporting proposed by Burton et al. [16], health vulnerabilities and social isolation were reflected in our 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. Participants appeared to be describing digital ageism in the form of *pervasive social attitudes* (or 'interpersonal biases' [19]).

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 [22, 23].

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' [24] Australia-based study found that victims' understanding of fraud was heavily influenced—and often exaggerated—by TV shows. They found that these programmes' depictions of special "sting" operations resulted in unrealistically optimistic expectations of law enforcement agency capabilities. One interviewee referenced TV as influencing his perception of perpetrators, suggesting media influences may have affected his reporting behaviour.

4.3. Clinical and Policy Implications. Shame around cybercrime victimisation has been attributed to pervasive ageist attitudes that blame older victims [25]. Such societal stigma could be tackled through the transmission of key messages to victims and nonvictims of all ages that challenge misconceptions surrounding victim gullibility or technological ineptitude. Our interviewees reported limited awareness of the support available to cybercrime victims, and benefits of disclosing victimisation to the police or bank, regardless of the scale. These messages are reflected in the UK Government's recent 'Stop! Think Fraud' public awareness campaign [26], which includes TV, radio and social media adverts, and a website with practical advice. This public information campaign is much needed. Our findings indicate that messages tailored and targeted to internet users with health and cognitive disabilities that may impede reporting would support its impact.

Several professional stakeholders mentioned the importance of neutral, trusted third parties such as charity workers or health and social care 'advocates' (i.e., individuals separate from the FJN or the authorities), who can guide and support victims through the reporting process. For socially isolated older adults experiencing poor mental or physical health in the UK, health and care professionals may be the only people they have contact with in-person. The potential role of home care workers as advocates for isolated older people has been highlighted [27]. Development of pathways and tailored advice will require multiagency collaboration, between health and social care organisations and the FJN, and their implementation buy-in from health and care and justice policymakers. Interviewees discussed the value of in-person, interactive, group sessions for older adults in community spaces, as one potential intervention modality. We propose that FJN organisations consider conducting a digital ageism assessment of their provisions to facilitate reporting by individuals of all age groups, in consultation with health and care agencies.

4.4. Limitations. There are a number of limitations to this study. Firstly, it is based on recall data, which is prone to bias and inaccuracy; victims of crime may forget or falsely recall events that occurred. Only older adults willing to disclose their victimisation to the researcher participated, so we 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 generalisability of findings relating to this group, but these data can be considered contextual. We 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 we were only able to access second-hand perspectives of their experiences from professional stakeholders. We 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. Our 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.

5. Conclusion

As cybercrime victimisation in older populations increases with increasing usage in this age group, it is critical to consider how to address the significant underreporting identified. Our research has uncovered a series of barriers to reporting—some of which are underpinned by interpersonal and corporate digital ageism—which serve as target areas for policymakers seeking to increase rates of disclosure. We propose next steps require multiagency collaboration across health and care and justice networks.

Data Availability Statement

Research data are not shared.

Ethics Statement

This study was approved by the UCL Research Ethics Committee (reference 25,325/001).

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

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.

Funding

This work was supported by the Dawes Centre for Future Crime at UCL.

Acknowledgements

We thank all participants for sharing their experiences and perspectives with us.

Supporting Information

Additional supporting information can be found online in the Supporting Information section. *(Supporting Information)*

Appendices 1-3 are topic guides used by the authors to guide and structure participant interviews. There is a tailored topic guide for each participant category. Appendix 1 is the topic guide for interviews with older adults who have been victims of cybercrime. Appendix 2 is the topic guide for interviews with professional stakeholders. Appendix 3 is the topic guide for interviewing friends and family.

References

[1] M. Daniel, "How Global Information Sharing Can Help Stop Cybercrime," *Harvard Business Review* (June 2023): https://hbr.org/2023/06/how-global-information-sharing-can-help-stop-cybercrime.

[2] Surfshark, "Cybercrime Statistics," *Surfshark* (2023): https://surfshark.com/research/data-breach-impact/statistics.

[3] C. S. J. Kung and A. Steptoe, "Changes in Internet Use Patterns Among Older Adults in England From Before to After the Outbreak of the COVID-19 Pandemic," *Scientific Reports* 13, no. 1 (2023): 3932, https://doi.org/10.1038/s41598-023-30882-8.

[4] C. Cross, "Theorising the Impact of COVID-19 on the Fraud Victimisation of Older Persons," *The Journal of Adult Protection* 23, no. 2 (2021): 98–109, https://doi.org/10.1108/JAP-08-2020-0035.

[5] K. Tripathi, S. Robertson, and C. Cooper, "A Brief Report on Older People's Experience of Cybercrime Victimization in Mumbai, India," *Journal of Elder Abuse & Neglect* 31, no. 4–5 (2019): 437–447, https://doi.org/10.1080/08946566.2019.1674231.

[6] J. Satchell, T. Craston, V. M. Drennan, J. Billings, and M. Serfaty, "Psychological Distress and Interventions for Older Victims of Crime: A Systematic Review," *Trauma, Violence, & Abuse* 24, no. 5 (2023): 3493–3512, https://doi.org/10.1177/15248380221130354.

[7] B. Havers, K. Tripathi, A. Burton, W. Martin, and C. Cooper, "A Qualitative Study Exploring Factors Preventing Older Adults From Reporting Cybercrime and Seeking Help," *CrimRxiv* (2024): https://doi.org/10.21428/cb6ab371.8c4e3181.

[8] R. Tarling and K. Morris, "Reporting Crime to the Police," *British Journal of Criminology* 50, no. 3 (2010): 474–490, https://doi.org/10.1093/bjc/azq011.

[9] Isaca, *State of Cybersecurity 2019* (2019), https://www.isaca.org/-/media/files/isacadp/project/isaca/why-isaca/surveys-and-reports/state-of-cybersecurity-2019-part-2_res_eng_0619.

[10] "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime1," *International Review of Law, Computers & Technology* 22, no. 1–2 (2008): 45–63, https://doi.org/10.1080/13600860801924907.

[11] A. Graham, T. C. Kulig, and F. T. Cullen, "Willingness to Report Crime to the Police: Traditional Crime, Cybercrime, and Procedural Justice," *Policing: International Journal* 43, no. 1 (2019): 1–16, https://doi.org/10.1108/PIJPSM-07-2019-0115.

[12] S. Giro Correia, "Making the Most of Cybercrime and Fraud Crime Report Data: A Case Study of UK Action Fraud," *International Journal of Population Data Science* 7, no. 1 (2022): 1721, https://doi.org/10.23889/ijpds.v7i1.1721.

[13] M. A. Abdulai, "Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud," *International Journal of Cyber Criminology* 14, no. 1 (2020): 157–174.

[14] K. Jaishankar, "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology," in *An International Perspective on Contemporary Developments in Victimology: A Festschrift in Honor of Marc Groenhuijsen*, eds. J. Joseph and S. Jergenson (Cham, Germany: Springer International Publishing, 2020), 3–19, https://doi.org/10.1007/978-3-030-41622-5_1.

[15] M. Bidgoli and J. Grossklags, "End User Cybercrime Reporting: What We Know and What We Can Do to Improve it," in *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (March 2016), 1–6, https://doi.org/10.1109/ICCCF.2016.7740424.

[16] A. Burton, C. Cooper, A. Dar, L. Mathews, and K. Tripathi, "Exploring How, Why and in what Contexts Older Adults Are at Risk of Financial Cybercrime Victimisation: A Realist Review," *Experimental Gerontology* 159 (2022): 111678, https://doi.org/10.1016/j.exger.2021.111678.

[17] M. Button, J. Tapley, and C. Lewis, "The "Fraud Justice Network" and the Infra-Structure of Support for Individual Fraud Victims in England and Wales," *Criminology and Criminal Justice* 13, no. 1 (2013): 37–61, https://doi.org/10.1177/1748895812448085.

[18] L. Ayalon and C. Tesch Römer, "Chapter 7 Introduction to the Section: On the Manifestations and Consequences of Ageism," in *Contemporary Perspectives on Ageism* (Cham, Germany: Springer Nature, 2018), 109, https://doi.org/10.1007/978-3-319-73820-8_7.

[19] A. Rosales, M. Fernández-Ardèvol, and J. Svensson, eds., *Digital Ageism: How it Operates and Approaches to Tackling it* (London, UK: Routledge, 2023), https://doi.org/10.4324/9781003323686.

[20] W. C. Adams, "Conducting Semi-Structured Interviews," in *Handbook of Practical Program Evaluation* (Hoboken, NJ: John Wiley & Sons, Ltd, 2015), 492–505, https://doi.org/10.1002/9781119171386.ch19.

[21] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide* (London, UK: SAGE Publications Ltd, 2021).

[22] J. Mariano, S. Marques, M. R. Ramos, et al., "Too Old for Technology? Stereotype Threat and Technology Use by Older Adults," *Behaviour & Information Technology* 41, no. 7 (2021): 1503–1514, https://doi.org/10.1080/0144929X.2021.1882577.

[23] W. Martin, G. Collett, C. Bell, and A. Prescott, "Ageing, the Digital and Everyday Life During and Since the Covid-19 Pandemic," *Frontiers in Psychology* 14 (2023): 1168340, https://doi.org/10.3389/fpsyg.2023.1168340.

[24] C. Cross and K. Richards, "The 'ACA Effect': Examining How Current Affairs Programs Shape Victim Understandings and Responses to Online Fraud," *Current Issues in Criminal Justice* 27, no. 2 (2015): 163–178, https://doi.org/10.1080/10345329.2015.12036039.

[25] C. Cross, "No Laughing Matter: Blaming the Victim of Online Fraud," *International Review of Victimology* 21, no. 2 (2015): 187–204, https://doi.org/10.1177/0269758015571471.

[26] Gov.Uk, "Stop! Think Fraud. Stop! Think Fraud," (2024), https://stopthinkfraud.campaign.gov.uk/.

[27] M. Leverton, A. Burton, J. Beresford-Dent, et al., "Supporting Independence at Home for People Living With Dementia: A Qualitative Ethnographic Study of Homecare," *Social Psychiatry and Psychiatric Epidemiology* 56, no. 12 (2021): 2323–2336, https://doi.org/10.1007/s00127-021-02084-y.

[28] B. Havers, K. Tripathi, A. Burton, S. McManus, and C. Cooper, "Research Note: Cybercrime Victimisation Among Older Adults: A Probability Sample Survey in England and Wales," *CrimRxiv* (2024): https://doi.org/10.21428/cb6ab371.46d2b268.