# “What a stupid way to do business”: Towards an Understanding of Older Adults’ Perceptions of Deceptive Patterns and Ways to Develop Resistance

KALYA WIN AUNG, EWAN SOUBUTTS, ANEESHA SINGH
UCL Interaction Centre, University College London, London, United Kingdom

There are growing efforts to reduce the harmful effects of deceptive patterns pervasively employed on e-commerce websites. However, efforts to produce new guidelines and introduce ethical design standards geared towards older adults have been limited. We investigate the potential of a serious game in fostering older adults’ resilience against manipulative designs in e-commerce through two studies. First, a survey with older adults ($N$ = 61), explored their attitudes towards deceptive patterns and identified characteristics influencing them. We then created a serious game, “Shopopolis”, to bolster older adults’ resistance to manipulative designs online and evaluated its efficacy with older adults ($N$ = 65). Our findings show that Shopopolis is a valuable tool for enhancing awareness, concern, and recognition skills related to e-commerce deceptive patterns. We discuss older adults’ unique perspectives on deceptive patterns and consider how insights can shape the design of targeted protective measures like Shopopolis for older adults in e-commerce contexts.

CCS Concepts: • **Human-centered computing → Empirical studies in HCI**; • **Human-centered computing** → HCI design and evaluation methods → User studies.

**Additional Key Words and Phrases:** Older adults, deceptive patterns, dark patterns, online manipulation, inoculation theory, serious and persuasive games, e-commerce, user experience, user interfaces

**ACM Reference Format:**
Kalya Win Aung, Ewan Soubutts, Aneesha Singh. 2024. “What a stupid way to do business”: Towards an Understanding of Older Adults’ Perceptions of Deceptive Patterns and Ways to Develop Resistance. *Proc. ACM Hum.-Comput. Interact.*, 8, CHI PLAY, Article 348 (October 2024), 30 pages, https://doi.org/10.1145/3677113

## 1 INTRODUCTION

The landscape of online shopping has so seamlessly integrated into our lives that we often overlook the factors driving our preferences for different e-commerce retailers. Yet, for retailers, such preferences hold great significance. To succeed in the industry, e-commerce retailers must deliver to users a compelling online shopping experience. However, there are instances when these attempts at persuasion straddle a fine line, venturing into the territory of consumer manipulation. Such design strategies, characterised by their manipulative intent [58], are dubbed “deceptive patterns”, previously referred to as “dark patterns”, and have become pervasive across online services [10,48,58]. Deceptive patterns not only capitalise on vulnerabilities in human psychology, but also exploit them to subvert consumers’ conscious decision-making [58]. Thus, they benefit the interests of technology companies at the expense of users [34].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
2573-0142/2024/10 – 348
© Copyright is held by the owner/author(s). Publication rights licensed to ACM.
https://doi.org/10.1145/3677113

Policymakers are increasingly concerned about the potential harms of deceptive patterns on individuals' autonomy, privacy, health, or economy [58]. For example, in e-commerce contexts [58], deceptive patterns can influence people to spend more time on shopping websites [88], impulsively buy more goods [39], or share their personal data with service providers for extra features [22,57]. Little attention has been paid thus far to user groups who may be disproportionately impacted by certain manipulative strategies, such as older adults [3,8,25,45,71].

Further, recent developments in the fields of privacy and security suggest that older adults have distinct privacy decision-making processes compared to younger adults [2], influenced by factors such as short-term memory, verbal fluency, and positive affect [25], which may significantly shape their perspectives and susceptibility to deceptive patterns. For example, some evidence suggests that older adults may not only be less likely to recognise manipulative attempts than younger people [8,45], but they may also be less aware that their behaviour online can be influenced [8]. Nonetheless, the specific deceptive pattern(s) to which older adults are more susceptible and effective interventions to mitigate their effects on older adults remain uncertain.

To resist the manipulative influence of deceptive patterns, past work shows that an individual must recognise the attempt at subversion and possess agency over it [8,9,55,64]. One approach to facilitate this concept may be to "inoculate" individuals against deceptive patterns. According to inoculation theory, people's resilience against persuasion attempts can be increased by increasing their understanding of the underlying techniques of the persuasive arguments [59]. Although this approach has never been explored as an intervention for deceptive patterns, a large body of research demonstrates the effectiveness of gamified approaches to inoculate individuals against online tactics to disseminate misinformation [5,6,54,82–84]. Gamified approaches enable 'active' inoculation, which is often more effective than traditional 'passive' inoculation approaches (e.g., reading campaigns) [4,26]. An example is "Bad News" [83], a gamified inoculation intervention that tasks players with creating content using misinformation techniques (e.g., forming echo chambers) from the perspective of fake news creators to build a fake news 'empire'. The game presents players with dichotomous choices (e.g., running attack ads or engaging in fact-focussed critique) to support them in countering arguments that challenge their existing beliefs. Researchers found evidence of the game's efficacy in reducing the perceived reliability and persuasiveness of fake news articles regardless of participants' age, gender, or education, highlighting inoculation theory as a potential tool to bolster resistance against deceptive patterns in older adults.

This paper explores how older adults perceive certain deceptive design practices and what mitigation strategies can be used to counteract them. First, through an exploratory survey using the deceptive pattern taxonomy derived by Mathur and colleagues [58], we investigated how older adults perceive different categories of deceptive patterns in terms of importance and concern. Based on these findings, we developed a prototype of a serious inoculation game, "Shopopolis", to raise awareness of deceptive patterns. Raising awareness and making older adults conscious of deceptive patterns they encounter is essential to engendering resilience against any patterns. We then conducted an evaluation study to assess if a serious game such as Shopopolis could increase older adults' awareness of the effect of deceptive patterns on their choices and behaviours, and whether (and how) playing Shopopolis can affect their ability to recognise deceptive patterns on shopping websites.

Findings from our exploratory survey reveal that older adults are affected by and concerned about restrictive, asymmetric, or hidden information deceptive patterns and encounter these frequently on shopping websites. Primarily, these fell into four main categories as described in

[58]: *Obstruction* (blocking access to functionality), *Forced Action* (requiring additional and tangential actions to complete a task), *Sneaking* (misrepresenting people's actions or hiding/delaying information that they would likely oppose), and *Misdirection* (steering people toward a choice using visuals or emotional language). Through Study 2, we focussed on educating older adults about these categories of deceptive patterns and demonstrated the effectiveness of a gamified inoculation intervention to counteract manipulative designs online. Use of Shopopolis with a group of 65 older adults reveals significant post-test increases in awareness, concern, and recognition ability of deceptive patterns on shopping websites.

We contribute understandings of deceptive patterns on the lives of older adults, the ways in which they respond to deceptive patterns individually, as well as avenues towards inoculating against deceptive patterns, through Shopopolis – our deceptive patterns intervention. Our findings encourage designers, developers, regulators, and educators alike to craft more targeted interventions for deceptive patterns, considering the specific digital inequalities that impact older adults.

## 2 RELATED WORK

### 2.1 Defining 'Deceptive Patterns'

"Deceptive patterns" is a term used to describe user interfaces that "trick users into doing things they might not otherwise do, such as buying insurance with a purchase or signing up for recurring bills" [15]. These patterns are used extensively and insidiously in online businesses to exploit people through carefully crafted 'tricks and traps'. This paper adopts Mathur et al.'s [58] framing for deceptive patterns as interface designs that employ manipulative strategies for competitive advantage. These designs often steer, nudge, coerce, or deceive people to engage in actions they may have refrained from if equipped with full attention, comprehensive information, absolute self-control, and unlimited cognitive capabilities. Deceptive patterns can differ in their design characteristics (e.g., covert, restrictive), design elements (e.g., text-based, visual-based), and their effects on people's autonomy, regulatory objectives, and individual or public welfare. Furthermore, differences emerge from the end-user's perspective, as individuals may consider certain types of deceptive patterns as more recognisable, resistible, or acceptable compared to others.

### 2.2 Deceptive Patterns in E-Commerce

Although deceptive patterns exist in a variety of web services, such as cookie banners [32,40,53,73,92], mobile applications [10,28,36,66,81], and gaming platforms [1,28,31,58,96,98], their use is perhaps most prevalent in e-commerce, i.e., a commercial way of making transactions online. Research suggests that many e-commerce websites incorporate deceptive patterns to influence customer behaviours [38]. Naturally, this influence has sparked concerns amongst experts regarding the potential harm caused to both individuals and companies [58]. For example, deceptive patterns can nudge people to spend considerable time using a service [48] (thus fuelling the so-called "attention economy" [42]), pressure people to shop more impulsively [55], and convince people to share their personal data [22,57]. Equally, e-commerce deceptive patterns can threaten collective welfare, eroding consumer trust in markets [7,48,86], promoting anticompetitive behaviour [24], and cause unforeseen societal consequences [58]. In this vein, deceptive patterns loom like shadows, exerting their influence across interactions at every level.

Unfortunately, research predicts the prevalence of deceptive patterns on e-commerce platforms to be high. In a 2019 study, Mathur et al. [57] identified 1818 instances of deceptive

patterns on over 11,000 online shopping websites, encompassing 15 types of deceptive patterns in 7 categories, including novel variations of previously identified manipulative techniques [15,34]. Notably, the most common of these categories was 'Scarcity', referring to deceptive patterns that manipulate the demand or availability of a product to amplify its desirability [41,51,72]. For example, a travel agent may display a prominent red banner warning *"Only 2 tickets left at this price!"*, urging quick purchases out of fear of missing out. Other categories of deceptive patterns in the authors' taxonomy included 'Urgency', 'Social Proof', 'Misdirection', 'Obstruction', 'Sneaking', and 'Forced Action', ordered by their observed prevalence. However, their automated approach only recognised overt, text-based deceptive patterns, leading the authors to note that their reported figures might be conservative-leaning as many visual and covert deceptive patterns could not be considered [57], indicating the potential for even higher prevalence of such practices.

More recently, a systematic component analysis of 200 top e-commerce websites in the U.S [68] found a minimum of 4 deceptive pattern features on each website that trigger impulse buying, where 75% of the websites employed at least 16 deceptive pattern features that nudged consumers toward impulse purchases. Thus, given the pervasiveness of deceptive patterns within e-commerce, the current paper focusses on shopping websites as a foundational domain.

### 2.3 Older Adults and Deceptive Patterns

Much HCI research on deceptive patterns stems from investigations into the perceptions and experiences of younger adults [7,33,48,55]. However, this narrow focus neglects other user groups who may be disproportionately affected by such designs. Older adults (aged 60 years plus, as per the UN definition [91]) are a prime demographic to study the effect of deceptive patterns on, as recent developments in the field of digital privacy and security suggest their attitudes, perspectives, and experiences with technology can make them more susceptible to the kinds of influence deceptive patterns present [75,79].

The prevailing narrative around older adults and online privacy tends to focus on older adults' difficulties keeping up with youth in handling digital interactions, such as managing their personal data [29,78], authentication [70], susceptibility to spam and spear-phishing [35,76], and preserving privacy [13]. However, HCI seeks to refrain from *'deficit-centric'* discourse around older adults' digital skills and cognitive abilities [93]. Instead, researchers argue that older adults simply have a different decision-making process, and thus encourage the design of technologies that cater to people's unique lived experiences. Knowles and Hanson [44] suggest that older adults' avoidance of technology stems from greater privacy concerns and, therefore, avoidance is an informed decision. However, Van den Broeck et al. [17] found that despite higher concern, this does not translate to more privacy protective actions, suggesting the presence of a privacy attitude-behaviour gap in older adults. Overall, while older adults are a heterogeneous group [94], such findings often lead scholars to conclude that they, on average, struggle more than other age groups with security and privacy challenges online [63].

Age-related disparities in privacy perceptions and behaviours may significantly shape how older adults interact with deceptive patterns in e-commerce. For example, design strategies may use nudges to make individuals disclose their data (e.g., through popups requiring an account to access deals, or 'Forced Action' [58]). Greater privacy concerns may also make older adults more cautious or resistant to disclosing personal information, and the attitude-behaviour gap might prompt initial caution but eventual compliance. Such differences in response may lead to distinct outcomes concerning privacy breaches, financial risks, or identity theft among older adults versus younger adults.

As these studies suggest, there is preliminary evidence that older adults face greater risks than other age groups from a variety of deceptive patterns online [3,45,71]. Bongard-Blanchy et al. [8] conducted a three-part survey to assess the impacts of deceptive patterns found on existing online services. Their study involving 413 participants concluded that an age below 40 constitutes a critical threshold for awareness and concern about the influence of deceptive patterns on behaviour, as well as the ability to recognise deceptive patterns. Koh and Seah [45] investigated the effects of: *'Low stock'* messages (i.e. limited product availability, or 'Scarcity' [58]), Activity Messages (showing activity on a website e.g., sales; 'Social Proof'), Countdown Timers (indicating when a deal will expire; 'Urgency'), and Limited-time Messages (indicating a deal will expire soon without a deadline; 'Urgency') on product selection decisions. They found that older adults are more susceptible to selecting products with these deceptive patterns than youth, making them more vulnerable to unintentional purchases online.

While vulnerability to deceptive patterns may increase with age, this effect might be pattern specific. Van Nimwegen and de Wit [71] experimentally investigated the relation between deceptive pattern recognition and platform choice, revealing a negative correlation between age and falling prey to "Sneak into Basket" (discretely adding items to someone's basket) and "Toying with Emotions" (persuading people through emotional language). Techniques are categorised under Mathur et al.'s [58] taxonomy as 'Sneaking' and 'Misdirection' respectively. Conversely, all age groups were equally likely to fall prey to "Trick Questions" (confusing people through language manipulation), classified under 'Misdirection' [58]. This suggests that the vulnerability of older adults to deceptive patterns is likely contingent on the type of deceptive pattern itself. In other words, it is not necessarily that older people are universally more susceptible or targeted than other groups; rather, the extent of their vulnerability may vary with their personal views of online activities, the deceptive technique employed, and the cognitive bias being exploited. It is therefore necessary to devise effective interventions and protective measures against deceptive patterns, which, in our first study, we delve into, to understudied distinctions in how older adults perceive, respond to, and potentially fall victim to deceptive patterns in e-commerce.

### 2.4 Intervention Spaces for Deceptive Patterns

Scholars have coined many intervention techniques for counteracting deceptive patterns. Emphasis has been placed on developing design measures, such as enforcing consent [37], hiding or disabling [46,50], adding friction [69], and using "bright patterns" [32]. Our research focusses on the potential of educational measures, which have seen little attention in literature.

Psychological inoculation is an awareness and education-based approach to developing cognitive resilience to persuasion attempts [19,20], which comprises two elements: *refutational pre-emption* and *threat. Refutational pre-emption* – or 'pre-bunking' – involves providing recipients with the information needed to resist the persuasive attempt [20], often including arguments or evidence that challenge the perspective presented in the attack (e.g., explaining that limited time offers often manipulate emotions rather than reflecting genuine scarcity). By applying the logic of inoculation to a deceptive pattern intervention, individuals should, in theory, be able to develop the cognitive resilience needed to better detect and counteract deceptive patterns on online shopping websites.

HCI researchers have proposed the use of gamification as an effective medium to apply inoculation theory [26]. Gamified approaches can provide 'active' inoculation, which is suggested to be more effective in promoting skill acquisition and information retention than traditional 'passive' inoculation approaches (e.g., reading campaigns) [4,26]. Evidence in favour of gamified inoculation largely stems from recent studies on tackling fake news online. Across a series of

experiments [54,82], participants completed pre- and post- test surveys to measure their ability to identify misinformation techniques used in news headlines and social media posts [54]. "Bad News" was a game based on inoculation mechanisms, such that participants were (a) directly forewarned about the dangers of fake news prior to gameplay i.e., *threatened* and (b) exposed to weakened doses of six misinformation techniques, encouraging critical reflection of the tactics e.g., *refutational pre-emption*. The results indicated that individuals in the Inoculation group, who played Bad News, demonstrated significantly improved accuracy in identifying false news compared to the Control group, who played Tetris [54]. Crucially for this research, the inoculation effect was found to remain stable for at least three months and was observed irrespective of age, underlining inoculation's educational potential.

In the second part of this paper, we extend this work by evaluating the efficacy of a similar gamified inoculation intervention, Shopopolis, in mitigating the impact of manipulative designs on shopping websites. To our knowledge, investigations have not focussed on the efficacy of this method for exploring deceptive patterns with the older adult demographic. Our aim therefore is to determine whether gamified inoculation can be used as a viable approach to increase older adults' awareness of deceptive tactics. Shopopolis deviates from previous applications of inoculation theory, as it does not counteract persuasive messages per se. Rather, its focus is on helping inoculate individuals against website design patterns that influence a particular behaviour. As Shopopolis teaches players how deceptive patterns on shopping websites work against their best interests, the assumption is that playing the game will result in greater awareness, concern, and recognition ability of these manipulation techniques.

## 3 STUDY 1: OLDER ADULTS' PERCEPTIONS OF DECEPTIVE PATTERNS

In our first study, we explore perceptions of deceptive patterns using survey data collected from older adult respondents.

### 3.1 Participants

Participants were recruited on a rolling basis for two weeks in June 2023 through convenience [90] and snowball [30] sampling. A survey link was shared via Reddit, WhatsApp, and Facebook. Eligible participants had to be: (1) Aged 60+, (2) A user of shopping or e-commerce websites, (3) Identify as a non-clinically vulnerable adult, (4) Able to provide informed consent, and (5) Able to communicate effectively in English.

Although 67 participants completed the survey, 6 of these participants were excluded from data analysis as they did not meet the age criterion. Therefore, 61 participants were included in data analysis. Most eligible participants were 60 to 75 years in age (55% 60-64, 27% 65-70, 4% 71-75), and 62% identified as women, 33% identified as men, 3% preferred not to disclose, and 2% preferred to self-describe.

### 3.2 Materials

The online survey was designed and distributed through a Qualtrics weblink. It was accessible on both mobile and web browser. Data was fully anonymised and participants' identifiable information was removed from their responses.

The survey consisted of 46 questions with 3 main sections. The first section probed basic demographic information about participants' age range and gender. In the second section, participants were presented with a description and example of one manipulative design technique from each of the seven categories of deceptive patterns identified in Mathur et al.'s [59] taxonomy,

informed by previous research on end-user perspectives of deceptive patterns [3,7,8,33,55]. They were asked questions about their experiences with and feelings towards each pattern. The final section probed into participants' gaming preferences, guided by past research on gamified inoculation and game design [82,84].

Prior to distribution, the survey questions were validated and refined through a pilot study with a small group of participants (not part of the older adult demographic) to ensure understanding, clarity, and alignment with the research objectives. The final survey questions are provided in Appendix A.

### 3.3 Procedure

A short description of the study rationale and link to the survey were shared on social media by the primary researcher. Participants who clicked the link were directed to an information sheet, which stated that the survey would take approximately 20 minutes, participation was entirely voluntarily, and respondents would not be compensated for their answers. Participants were informed that they were consenting to the use of their data by continuing with the survey and submitting their responses. After completing the survey, respondents were thanked for their participation.

### 3.4 Data Analysis

Incomplete survey responses ($N = 31$) were removed from data analysis as informed consent could not be assumed. For the closed-ended questions, quantitative analysis was performed using SPSS to yield descriptive statistics. Since these questions were mandatory, this analysis covered the entire participant sample ($N = 61$). All survey data was anonymous, and any identifiable details that may have been added by participants were removed from open-ended responses before analysis. The study was approved under the following ethics code: UCLIC_1920_007_Staff_Singh.

An inductive reflexive thematic analysis [14] was conducted by the first author on both the mandatory open-ended questions and optional open-ended questions where participants provided responses. The author first familiarised themselves with the dataset, reading through all survey responses twice and taking initial notes. Using NVivo, the first ten participant responses were open coded [14] to identify patterns related to participants' attitudes and experiences with deceptive patterns. This first round of open coding generated a set of initial codes. The author then continued open coding the remaining responses, comparing new data with existing codes and adding new codes as patterns emerged, and grouping similar codes into higher-level codes, such as "Avoidant Behaviour" mapped to the higher-level code "Behavioural Response". Higher-level codes were discussed and refined with co-authors, and affinity mapping was applied to develop four overarching themes from these higher-level codes. For example, "Behavioural Response" was mapped to the theme of "Lack of Transparency and Trust", as participants' avoidance of deceptive patterns often indicated a lack of trust in these e-commerce platforms. All authors iterated on these themes twice to ensure that every open-ended response was captured by at least one theme and reflected on Mathur et al.'s [58] structure during the write-up process. A detailed codebook, mapping out the initial codes and higher-level codes derived from the data, is provided in Appendix B.

### 3.5 Survey Results

*3.5.1 Overview of Survey Metrics.* Fig. 1 provides a graphical overview of key survey results. Most participants reported encountering deceptive patterns on shopping websites often (66%) or sometimes (25%). None of the participants reported never encountering a deceptive pattern

before, however only around a quarter (26%) of participants were familiar with the concept of deceptive patterns prior to completing the survey.

With reference to the 7 deceptive patterns included, Hard to Cancel and Forced Enrolment were most commonly encountered (84%), followed closely by Confirmshaming and Activity Notifications (80%), Deceptive Countdown Timers (79%), and Hidden Costs (77%). High-demand messages, although less frequently encountered, were still reported by almost two-thirds (66%) of participants.

Almost one-third (32%) of participants rated Hidden Costs and Hard to Cancel as the joint most concerning and important deceptive patterns to be able to identify when shopping online. Forced Enrolment (17%) was the next most concerning deceptive pattern for participants. High-demand messages (6%), Deceptive Countdown Timers (5%), and Confirmshaming (5%) received a similar minority percentage of selections. Finally, Activity Notifications (4%) was perceived as the least concerning and important pattern for participants to identify online.

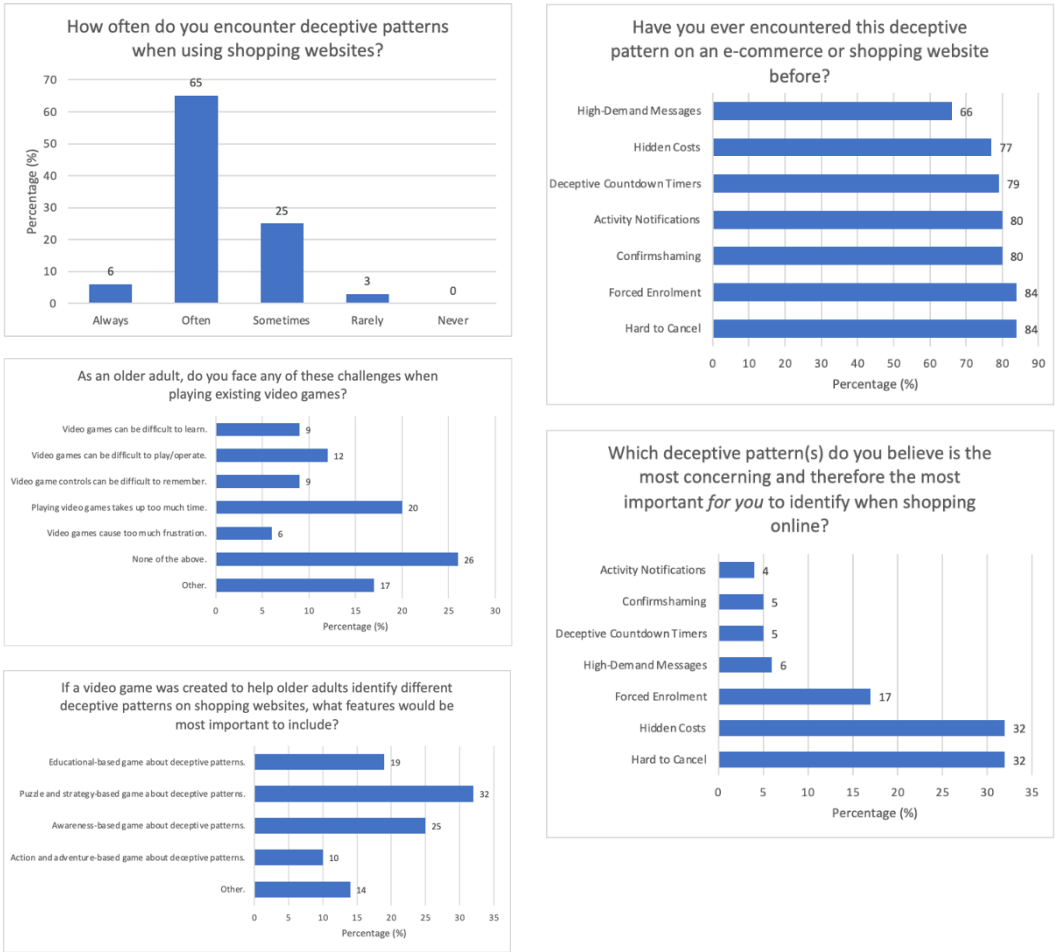



Fig. 1. Graphical overview of findings from exploratory survey

Regarding the third section of the survey about video games, three-quarters (75%) of participants reported that they currently play or have played a video game before. When asked

to envision a potential video game to help older adults identify deceptive patterns on shopping websites, most reported a preference for a puzzle- and strategy- based game (31%), an awareness-based game (26%), or an educational-based game (20%) about deceptive patterns.

*3.5.2 Overview of Survey Responses.* A thematic analysis of the qualitative survey responses led to four themes being identified: (1) Lack of Transparency and Trust; (2) Knowledge and Recognition of Deceptive Patterns; (3) Asserting Personal Agency and Decision-making; and (4) Learned Strategies to Overcome Deceptive Patterns. P# is used as a participant identifier for survey participants.

*3.5.3 Lack of Transparency and Trust.* In exploring the impact of deceptive patterns on older adults, participants voiced concerns about the honesty and integrity of e-commerce platforms that employ such tactics. Among these patterns, Hard to Cancel stood out as particularly frustrating. Some participants found the call-to-cancel practice excessively time-consuming, noting that it would take *"half a lifetime to cancel/discontinue [the service/transaction]"* (P50) so that companies could *"try to keep you [as a customer for longer]"* (P43). Others felt anger due to unclear pricing, hidden costs, or misleading subscription details leading to unintended financial commitments (P29). Confirmshaming, a deceptive tactic that induces guilt to influence user choices, caused confusion among some participants, which negatively influenced their decision-making process (P53).

Interestingly, while there was a prevalent negative perception of deceptive patterns, not all participants viewed them unfavourably. Some admitted that they had never perceived certain patterns as "*deceptive or somehow 'bad'*" (P9) and even found humour in the overt nature of tactics like Deceptive Countdown Timers (P58). Despite this range of emotional responses, participants' behavioural reactions to deceptive patterns were similar, often involving clicking away from or completely exiting the website. This avoidant behaviour seemed most pronounced for deceptive patterns characterised as restrictive by Mathur and colleagues [58] such as Hard to Cancel (*"If I know it will be hard to cancel, I won't sign up"*; P45) and Forced Enrolment (*"I just click away [from the Forced Enrolment popup] and Google the story"*; P9). These patterns, encompassing actions like offering inconvenient cancellation options and mandating account creation for website access, both limit the set of choices available to complete a task.

Participants emphasised the importance of clear and honest communication from websites to build trust among older adults, such as presenting transparent cancellation instructions when signing up to a service (P34). As participants encountered more deceptive patterns, they grew privy to the companies employing these tactics, leading to a preference for only *"a handful of trusted sites"* (P13). This trend suggests that repeated exposure to deceptive patterns might erode trust in e-commerce platforms over time, prompting individuals to become more cautious in their online engagements.

*3.5.4 Knowledge and Recognition of Deceptive Patterns.* Participants held varying perceptions regarding the underlying motives behind deceptive patterns. Broadly, participants were aware of the manipulative intent embedded within deceptive patterns *("I knew it was manipulation"*; P18). However, not all participants perceived these features as manipulative. Some interpreted them as benign marketing techniques aimed at encouraging purchases (*"[...] just thought these were marketing ploys to make you feel like you have to purchase some"*; P57), while a minority even considered them helpful ("*I thought it [Hidden Costs] helped to show me where to click!*"; P28).

Deceptive patterns that hid information from individuals, such as Hidden Costs and Hard to Cancel, were difficult for participants to detect early on. Participants expressed that the manipulative aspects of these patterns only became evident when they attempted to interact with them, making them *"difficult to identify [...] until you need to use [them]"* (P25). Age-related factors

influenced perception, with older adults displaying more caution toward patterns with potential long-term effects (*"I don't want to leave subscriptions for others to end"*; P16).

Participants emphasised the importance of visibility, advocating for larger screens and legible fonts. Increasing awareness of deceptive practices was also viewed as essential in identifying these patterns (*"Just being aware that it [Deceptive Countdown Timers] is a deceptive practice will help"*; P31).

*3.5.5 Asserting Personal Agency and Decision Making.* Older adults expressed the desire to make choices based on their needs and preferences, rather than being influenced by the shopping interface. This sentiment was reflected in opinions of each deceptive pattern. Patterns that possessed restrictive characteristics, such as Hard to Cancel and Forced Enrolment, were considered the least acceptable by many as they overtly limit people's choices (P4). Conversely, patterns exploiting social biases like the Bandwagon Effect – the tendency of individuals to place higher value on something due to its popularity among others [87] – were perceived as more acceptable, as participants believed in their ability to be *"resistant"* (P42) to such persuasion.

Participants preferred platforms that respected their autonomy and provided transparent information to support their decision-making process. However, acceptance of manipulative practices was often contingent on the company's reputation. For example, P29 felt more forgiving towards a well-known reputable site that required membership to browse, but criticised a new company for employing the same tactic, stating, *"I've never even heard of you and you're hiding your merch from me? What a stupid way to do business"*. Additionally, cost played a role in perceptions, with some participants willing to overlook deceptive patterns if it meant receiving *"the best deal"* (P29).

*3.5.6 Learned Strategies to Overcome Deceptive Patterns.* Participants used various strategies to counter the influence of different deceptive patterns. When encountering restrictive patterns aimed at limiting options (i.e., Hard to Cancel and Forced Enrolment), participants often avoided these platforms entirely (P39) or carefully read the terms and conditions prior to committing to a service (P12). Others proactively set calendar reminders to cease Hard to Cancel subscriptions before the billing period began.

For asymmetric patterns designed to create unequal choices (i.e., Confirmshaming and Forced Enrolment), participants ignored emotionally charged language and avoided selecting options presented in a coercive manner. P42 described using a *"dedicated 'spam' e-mail address"* when signing up for a website's newsletter to access exclusive deals.

When faced with covert patterns that influence decisions without the person's knowledge (i.e., Deceptive Countdown Timers, Activity Notifications, and High-demand Messages), many critically evaluated the given information. For Activity Notifications, participants often assessed the authenticity of the activity portrayed (*"I look at the numbers and decide if they have any truth. If it's unlikely I pass"*; P44). Some also expressed a habit of cross-referencing product availability claims across websites before deciding. Others deliberately waited a day or more before purchasing, regardless of timer or stock level indicators, in hopes of receiving a discount (P48).

To overcome deceptive patterns (i.e., Hidden Costs, Deceptive Countdown Timers, and Activity Messages) and information-hiding patterns (i.e., Hidden Costs and Hard to Cancel), participants evaluated all information presented before making a purchase, considering factors like *"shipping and convenience fees"* (P43) and utilising cost-comparison methods or third-party shopping tools (P42) to secure the most favourable deal.

## 4 DESIGNING SHOPOPOLIS

In this section, we introduce the design of Shopopolis: A novel inoculation game designed to enhance older adults' awareness of manipulative interface design. To begin, we demonstrate how Shopopolis was designed and prototyped based on formative findings from our survey data in Study 1. We then present a second investigation assessing the impact of playing Shopopolis on older adults' awareness of and concern about the influence of deceptive patterns, as well as their ability to recognise such patterns on shopping websites.

### 4.1 Design of Shopopolis

Our thematic analysis revealed three key design takeaways from the survey in Study 1. First, results suggested that Obstruction, Sneaking, Forced Action, and Misdirection were the most prevalent and concerning categories of deceptive patterns encountered by older adults during online shopping. Second, although every older adult reported previously encountering deceptive patterns on e-commerce websites, most were unaware of the concept and term 'deceptive patterns' prior to completing the survey. Finally, older adults generally had an affinity towards strategy- and awareness- based video games, especially in comparison to action- and adventure-based video games.

In response to these findings, Shopopolis draws on the second and third key takeaways from Study 1 in a serious game format and targets: (1) lack of awareness of deceptive patterns we found among most older adults, and (2) the preference for strategy- and awareness- based video games within the older adult demographic. Related work highlighted the efficacy of games as a medium for applying active inoculation theory on older adults [5,54,82]. Additionally, gamification can enhance skill acquisition and information retention more than traditional passive approaches [12,21,23,80,97].

To address the first design takeaway from Study 1, Shopopolis comprises four levels dedicated to the deceptive pattern categories – Obstruction, Sneaking, Forced Action, and Misdirection – that were rated as highly concerning and frequently encountered by older adults. In the game, players take on the role of a recently appointed design lead at an up-and-coming e-commerce company. Similar to real-world e-commerce practices, their primary goal is to maximise total sales by implementing website features that enhance user engagement. Fig. 2 illustrates one such feature included in the game. Players are rewarded with sales if they choose designs incorporating deceptive patterns taught in the game (see Fig. 3). Conversely, players are punished with lower user engagement (and therefore lower sales) when choosing designs that prioritise honesty and transparency (see Fig. 4). To provide an authentic experience aligned with older adults' real-life encounters on e-commerce websites, Shopopolis inoculates players against deceptive design features and scenarios described by participants in Study 1, such as coercing people to call to cancel (P43).

The first level, "Misdirection", educates players on how shopping websites use visuals, language, and emotion to manipulate perceptions of product value, often exploiting the Anchoring Bias [57,58]. The second level, "Sneaking", covers techniques that hide crucial information – such as adding unwanted items to one's cart – to manipulate people without their knowledge or consent. Players are taught how shopping websites exploit the Default Bias and Sunk Cost Fallacy to encourage people to continue their engagement despite potential drawbacks [43,48,58]. The third level, "Forced Action", players learn about more extreme deceptive patterns, such as mandatory account creation and sharing features, and how these manipulate people into taking specific actions they may not choose voluntarily. The final level, "Obstruction", focusses

on deceptive patterns that make it exceedingly difficult for people to disengage from the website once they are on it. These tactics include forcing people to navigate through numerous steps or hiding cancellation options, all with the intention of keeping them hooked and preventing them from leaving the site easily [15,16,58].

Shopopolis was designed to include the two components necessary for psychological inoculation to occur [59,61]. First, *refutational pre-emption* is addressed by urging players to consider the impact of deceptive patterns on people's behaviour and explore less manipulative redesign options. Second, the game deliberately creates tension between user engagement and agency to evoke an unsettling emotional response, as players must take responsibility for exploiting people's decision-making (shown in Fig. 5, depicting one scenario where players are educated about the consequences of implementing a Hard-to-Cancel feature).

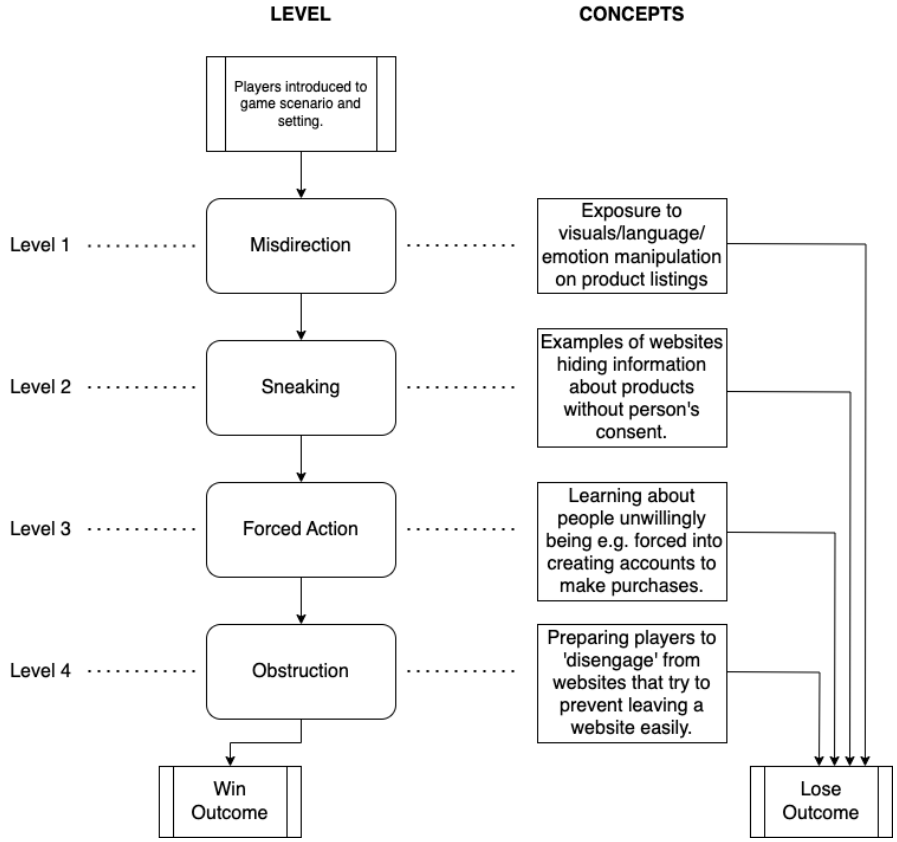



Fig. 2. Overview of Shopopolis game completion states.

Shopopolis was piloted with a small sample of three older adults, who played through an early Figma prototype. Initial feedback indicated that all players found the user interface visually appealing, felt more aware of deceptive patterns, and felt better prepared to identify and avoid deceptive patterns in real-life scenarios. Feedback also highlighted participants' desire for more significant consequences and stakes to increase their emotional investment in the game. In response to this feedback, the game was iterated so that if the engagement dial falls too low, players lose their job at the business and must redo the level. Fig. 6 depicts a situation where players must change their mind so as not to lose the game. The final Figma prototype of Shopopolis is available to be viewed at this link: https://shorturl.at/HIPQ1.


Fig. 3. Feature implementation

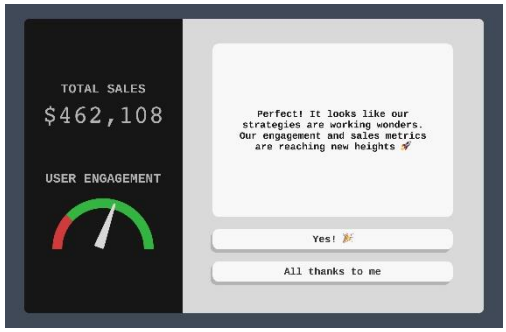



Fig. 4. Result of choosing a manipulative feature

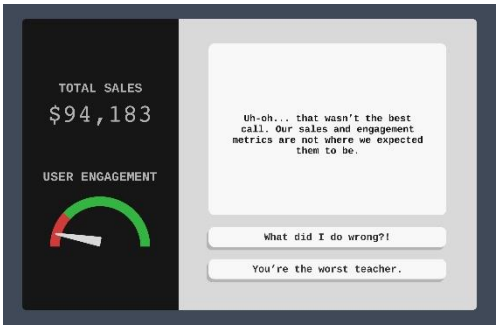



Fig. 5. Result of choosing a non-manipulative feature

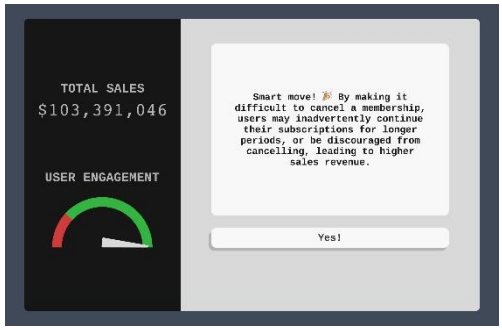



Fig. 6. Teaching players about cognitive biases

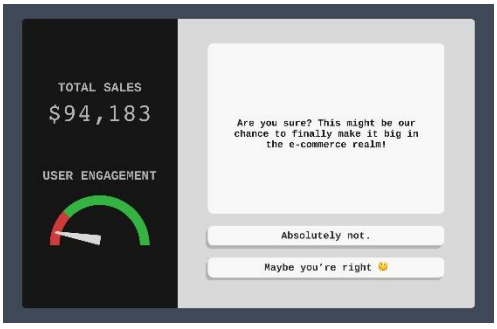



Fig. 7. A decision that may result in game loss

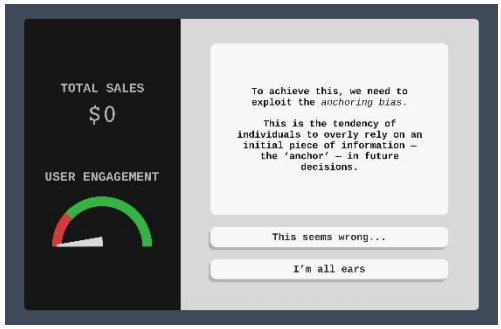



Fig. 8. Teaching players how deceptive patterns work against their best interests

## 5 STUDY 2: EVALUATING SHOPOPOLIS

### 5.1 Participants

Participants were recruited in July 2023 via Prolific (https://www.prolific.co), a crowdsourcing platform acknowledged for its data quality [77]. As in Study 1, participants had to be: (1) Aged 60+, (2) Shopping online at least once every few months on average, (3) Identify as a non-clinically vulnerable adult, (4) Able to provide informed consent, (5) Fluent in English, and (6) Had a perfect approval rate (i.e., never failing a study) on Prolific. In exchange for their time, all participants received monetary compensation worth $3.04, in line with Prolific's recommended hourly rate.

A total of 66 participants completed the experiment. After employing data quality checks to identify participants who did not pass the attention filter (i.e., failing to input the correct video game completion code), the sample was reduced to 65 participants. Of these, 52% identified as men and 48% identified as women. Most participants were aged between 60 to 64 years (32% 65-70, 11% 71-75, 3% 76-80). Their education level ranged from less than a high school diploma to a post-graduate degree, with the modal education representing completion of a bachelor's degree (32%).

| Category | Type (Number of Shopping Interfaces in the STDP Task that employed this Deceptive Pattern) | Description | Asymmetric? | Covert? | Deceptive? | Hides Info? | Restrictive? | Cognitive Biases |
|---|---|---|---|---|---|---|---|---|
| **Sneaking** | Sneak into Basket (x1) | Adding additional products to people's shopping carts without their consent | Never | Never | Sometimes | Always | Never | Default Effect |
| | Hidden Costs (x1) | Revealing previously undisclosed charges to individuals right before they make a purchase | Never | Never | Sometimes | Always | Never | Sunk Cost Fallacy |
| **Misdirection** | Confirmshaming (x1) | Using language and emotion (shame) to steer people away from making a certain choice | Always | Never | Never | Never | Never | Framing Effect |
| | Visual Interference (x1) | Using style and visual presentation to steer people to or away from certain choices | Sometimes | Always | Sometimes | Never | Never | Anchoring & Framing Effect |
| **Obstruction** | Hard to Cancel (x2) | Making it easy for someone to sign up for a service but hard to cancel it | Never | Never | Never | Sometimes | Always | None |
| **Forced Action** | Forced Enrolment (x2) | Coercing people to create accounts or share their information to complete their tasks | Always | Never | Never | Never | Always | None |

Table 1. Deceptive patterns used in the STDP Task [58]

### 5.2 Design and Materials

Study 2 tested a prototype of Shopopolis built using Figma (https://www.figma.com). The experiment manipulated condition as a between-subjects variable: Participants either played

Shopopolis (Inoculation) or Tetris (Control). Based on the three-part survey methodology of Bongard-Blanchy and colleagues [8], the dependent variables were awareness of influence, awareness of potential harm, worries about manipulative design, and deceptive pattern detection score. These variables were measured both pre- and post- game intervention. participants received monetary compensation worth $3.04, in line with Prolific's recommended hourly rate.

*5.2.1 Awareness and Concern Scale.* The pre- and post- test measures of awareness and concern included items taken from Bongard-Blanchy et al.'s [8] study on deceptive patterns from an end-user perspective. Six statements were displayed in pairs (one pair per page) opposing personal perspective ("my/me") and general perspective ("people/others"). These measured participants' awareness of influence, awareness of potential harm, and worries about manipulative design. Participants rated their agreement using a 5-point Likert scale (-2 = *strongly disagree*; 2 = *strongly agree*).

*5.2.2 Spot-the-Deceptive-Pattern (STDP) Task.* To evaluate participants' ability to recognise various deceptive pattern types, a pre- and post- assessment was adapted from Bongard-Blanchy's [8] study. Ten e-commerce website interfaces were displayed in a random order, with any reference to real companies digitally removed by the researcher. Two control conditions without any deceptive patterns were included. The other eight interfaces contained deceptive patterns from one of the four categories included in the game of Shopopolis, such that there were two examples for each deceptive pattern category. Table 1 summarises the deceptive patterns used in this task, organised according to Mathur et al.'s [58] taxonomy.

As in Bongard-Blanchy et al. [8], each interface was presented for 10 to 30 seconds based on the degree of textual complexity. Participants were asked if they noticed any design element that could influence their behaviour. Crucially, it was explicitly stated beforehand that not all interfaces would contain such elements. This indication and the time restriction served to prevent excessive searching that is not natural to real-life online shopping contexts. After each interface disappeared, a thumbnail of the interface and a text field was displayed, where participants were asked to describe the manipulative element (i.e., means of influence) and the presumed service intention (i.e., its purpose). See Appendix C for all interfaces included in this task.

### 5.3 Procedure

Following consent, participants were presented with demographics questions, the Awareness and Concern Scale, and the STDP task to record baseline values. Participants were then randomly allocated to either the Inoculation ($N$ = 30) or Control ($N$ = 35) group. Those in the Inoculation group played Shopopolis until completion. To prove that they had completed the entire game, participants were required to enter a code displayed on the final game screen to proceed with the experiment. The Control group played Tetris for 8 minutes (the average time to finish Shopopolis in the pilot study). Tetris was chosen to control for the game modality of Shopopolis. This aligns with our focus on investigating the effects of gamified (active) inoculation, which past research suggests is superior to passive inoculation in supporting learning [4,26]. Therefore, comparing Shopopolis with a passive non-game inoculation, such as passively presenting information about deceptive patterns, would not be appropriate for our study. Next, both groups completed the Awareness and Concern Scale and the STDP task again to record post-intervention data. Participants were finally thanked for their participation.

### 5.4 Data Analysis

To analyse data gathered from the Awareness and Concern Scale, dependent sample statistical tests were conducted. Pre- and post- intervention responses from within-subjects Likert scale

items were analysed on SPSS using the Wilcoxon matched-pairs signed-rank test. *P*-values less than 0.05 were deemed significant. For Likert data, median over mean was used as a measure of central tendency due to the ordinal nature of Likert items.

Similar to [8], the free-text descriptions of each interface from the STDP task were hand-coded using a deductive approach. Specifically, participants were assigned a score based on whether they identified the manipulative design element(s) correctly from Mathur et al.'s [58] description of the deceptive patterns (no = 0 / partly = 0.5 / yes = 1). Although each interface (excluding the two controls) contained one main deceptive pattern, further possible manipulative elements identified by participants were inductively added into the pool of correct or partly correct answers. All responses were blindly coded in Microsoft Excel by the first author. The pre- and post- intervention deceptive pattern detection scores for each participant were summed (ranging from 0 to 10). After confirming the normality assumption, paired samples *t*-tests were conducted on these scores in SPSS to determine whether there were any changes in recognition performance before and after the intervention for each condition. An independent sample *t*-test was conducted on the difference in pre- and post- intervention detection scores to determine whether this change was higher in the Inoculation or Control condition.

### 5.5 Post-Inoculation Results

Below, we present the findings from players of the Shopopolis inoculation game. These are presented here as participants' awareness of different outcomes, shown quantitatively. As descriptive statistics revealed, participants in both conditions generally agreed with all six Likert statements. This was true for pre- *and* post- intervention ratings, with medians ranging from neutral (0) to strongly agree (+2) across conditions. Table 2 summarises the descriptive data for the Awareness and Concern Scale.

| Likert Item | | Inoculation | | | | Control | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Pre-Intervention** | | **Post-Intervention** | | **Pre-Intervention** | | **Post-Intervention** | |
| | | **Median** | **IQR** | **Median** | **IQR** | **Median** | **IQR** | **Median** | **IQR** |
| Awareness of Influence | **General** | 2.00 | 1.00-2.00 | 2.00 | 2.00-2.00 | 1.00 | 1.00-2.00 | 2.00 | 2.00-2.00 |
| | **Personal** | 1.00 | .75-1.25 | 1.00 | 1.00-2.00 | 1.00 | .00-1.00 | 1.00 | 1.00-1.00 |
| Awareness of Potential Harm | **General** | 1.00 | .00-2.00 | 2.00 | 1.00-2.00 | 1.00 | 1.00-2.00 | 1.00 | 1.00-2.00 |
| | **Personal** | .50 | -1.00-2.00 | 1.00 | .00-2.00 | 1.00 | -1.00-1.00 | 1.00 | 1.00-1.00 |
| Worried about Manipulative Designs | **General** | 1.00 | .00-2.00 | 2.00 | 1.00-2.00 | 1.00 | .00-1.00 | 1.00 | 1.00-2.00 |
| | **Personal** | .50 | -1.00-1.25 | 1.00 | .00-2.00 | 0.00 | -1.00-1.00 | 1.00 | 1.00-1.00 |

Table 2. Descriptive statistics for Awareness and Concern Scale

Wilcoxon matched-pairs signed-rank tests were conducted on each of the three statement pairs to determine if there was a significant change in pre- and post- intervention median scores. In this test, each participant is compared with themselves, and changed scores are compared in a ranked analysis. Table 3 provides an overview of the within-groups comparisons for this measure.

| Likert Item | | Inoculation ($N$ = 30) | | | | Control ($N$ =35) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | **Higher ($N$)** | **Lower ($N$)** | **Ties ($N$)** | ***p*-value** | **Higher ($N$)** | **Lower ($N$)** | **Ties ($N$)** | ***p*-value** |
| Awareness of Influence | **General** | 6 | 1 | 23 | .206 | 7 | 2 | 26 | .248 |
| | **Personal** | 10 | 2 | 18 | .019 | 10 | 6 | 19 | .872 |
| Awareness of Potential Harm | **General** | 14 | 1 | 15 | .001 | 5 | 5 | 25 | .589 |
| | **Personal** | 14 | 2 | 14 | .006 | 5 | 6 | 24 | .813 |
| Worried about Manipulative Designs | **General** | 14 | 1 | 15 | .001 | 11 | 1 | 23 | .005 |
| | **Personal** | 13 | 4 | 13 | .013 | 11 | 2 | 22 | .012 |

Table 3. Wilcoxon tests for Awareness and Concern Scale

*5.5.1 Awareness of influence.* The first statement pair assessed participants' awareness of the influence of deceptive patterns online ("The design of websites or applications can influence [people's/my] choices and behaviours."). The Wilcoxon matched-pairs signed-rank test revealed that when framed from a general perspective ("people"), participants in both the Inoculation condition ($N$ = 30) and Control condition ($N$ = 35) did not alter their views on the statement following the intervention. However, in the Inoculation condition, there was a significant increase in awareness of potential personal influence ("my") after playing Shopopolis ($p$ = .019), while the Control group's awareness remained unchanged. These results suggest that Shopopolis effectively increased participants' awareness of how deceptive patterns can influence their own online behaviour but had no impact on their views of how these patterns might influence others' behaviour. The research hypothesis was thus partially supported.

*5.5.2 Awareness of potential harm.* As we showed through the outcomes of Study 1, participants had varying levels of ability to detect deceptive patterns. Regarding the second pair of statements ("Websites or applications that are designed to manipulate users can cause harm to [people/me]."), there was a significant increase in awareness of harm in the Inoculation condition for both general ($p$ = .001) and personal ($p$ = .006) perspectives. This indicates that Shopopolis effectively strengthened participants' negative views about the potential detrimental effects of deceptive patterns on themselves and others. The Control condition experienced no change in awareness of harm for either perspective. The research hypothesis was fully supported.

*5.5.3 Worries about manipulative designs.* For the final statement pair ("I am worried about the influence of manipulative websites and applications on [people's/my] choices and behaviours."), the Wilcoxon test revealed significantly higher post-intervention ratings of concern in the Inoculation group (general: $p$ = .001; personal: $p$ = .013). Interestingly, this increase in concern was also observed for both perspectives in the Control group (general: $p$ = .005 personal: $p$ = .012). These findings suggest that the heightened awareness observed in the first two statement pairs indeed translated into increased concerns after playing Shopopolis. This also contrasts Study 1's finding regarding older adults valuing clear and honest communication to establish trust. It was unclear how those who previously found deceptive patterns to be 'amusing' or 'humor[ous]' were also affected by the inoculation. However, this increase in concern was not exclusive to the Inoculation group. The research hypothesis was therefore only partially supported.

*5.5.4 Within-group comparisons of deceptive pattern detection score.* To assess the impact of Shopopolis on improving participants' ability to recognise deceptive patterns, a paired samples *t*-

test was computed comparing the mean pre- and post- intervention deceptive pattern detection scores of the Inoculation group. The pre-intervention mean score ($M$ = 3.78, $SD$ = 2.09) and the post-intervention mean score ($M$ = 5.42, $SD$ = 2.19) revealed a statistically significant increase in the recognition ability of older adults after playing Shopopolis ($t$ = -5.64, $df$ = 29, $p$ < .001 2-tail). The research hypothesis was thus supported. As for the Control group, analysis of the pre-intervention mean score ($M$ = 4.24, $SD$ = 2.12) and the post-intervention mean score ($M$ = 4.66, $SD$ = 1.93) showed no difference in recognition ability after playing Tetris ($t$ = -1.74, $df$ = 34, $p$ = .090 2-tail), supporting the research hypothesis. Table 4 presents findings from the paired $t$-tests for both conditions.

*5.5.5 Recognition improvement comparisons between Inoculation and Control group.* To compare the degree of deceptive pattern recognition improvement between conditions, change scores (i.e., the difference in pre- and post- intervention detection scores) were calculated for each participant. Mean change scores for the Inoculation group ($M$ = 1.63, $SD$ = 1.59) and the Control group ($M$ = .41, $SD$ = 1.41) were then subjected to an independent samples $t$-test. Consistent with the research hypothesis, the Inoculation group had significantly higher increases in detection scores from pre-intervention to post-intervention compared to the Control group, $t(63) = 3.28$, $p$ = .002 2-tail. This indicates that participants who played Shopopolis experienced more substantial improvements in recognising deceptive patterns than those who did not engage in the game. This also contrasts with participants' survey responses, indicating that their subjective impressions of self-confidence pre-inoculation may be unfounded.

## 6 DISCUSSION

We conducted two studies exploring end-user perceptions of e-commerce deceptive patterns, focusing specifically on adults aged sixty and above. Evaluating Mathur et al.'s [58] taxonomy as a descriptive and comparative framework for understanding the relationships between deceptive patterns and older adults' responses showed that restrictive or hidden information deceptive patterns were the most frequently encountered by older adults on shopping websites and were also perceived as the most concerning (P3,4,16,25,30,43,52). These deceptive patterns included those classified by Mathur et al. [58] under Obstruction, Forced Action, and Sneaking. The second study showed that Shopopolis successfully induced an inoculation effect in older adults, increasing their awareness of, concerns about, and abilities to recognise deceptive patterns on shopping websites. In this section, we explore how these findings have the potential to further discussion of the effect of deceptive patterns on older adults, and the potential for inoculations like Shopopolis in developing deceptive pattern interventions in the future.

### 6.1 Mitigating the Effects of E-Commerce Deceptive Patterns for Older Adults

Even though the term 'deceptive pattern' was unknown to almost two-thirds of participants, the results of Study 1 show that they were somewhat aware of the existence of such techniques and recognised some presented examples, which is in line with past evidence indicating a growing general awareness of deceptive patterns among older adults [3,8,33]. Out of the seven examples of deceptive patterns tested in Study 1, Hard to Cancel and Forced Enrolment were most frequently encountered by respondents when shopping online. This is in contrast to Mathur et al.'s large-scale web crawl study where these patterns were some of the least observed, suggesting a disparity between the prevalence of deceptive patterns in real-world online encounters and the reported awareness among older adults. For HCI researchers, this observation implies that addressing manipulative design extends beyond simply counting occurrences or assessing

awareness. Rather, it highlights the importance of understanding the cognitive and emotional mechanisms older adults employ when confronted with deceptive patterns. Consequently, the design of e-commerce sites should be considerate of older adults who, are more susceptible to being influenced [8] and may struggle to adapt their self-protection strategies online [11].

There is potential for a further mitigation of the effects of deceptive patterns online, by exploring, for example, how participants in Study 1 exhibited stronger emotions towards certain types e.g., information hiding deceptive patterns. HCI researchers could explore this avenue further to understand whether emotional resonance influences the visibility of different deceptive pattern types in older adults, paving the way for more tailored educational efforts.

Study 1 also shed light on the interplay between deceptive pattern prevalence and user acceptance. It has been assumed within the literature that initial anger or annoyance towards deceptive patterns reduces as exposure increases, akin to the gradual normalisation of an intrusive salesman's tactics [33,55]. However, in our study, the deceptive patterns Hard to Cancel and Forced Enrolment were also rated as the most concerning, alongside Hidden Costs, as shown by P3,4,25,39,52. For some older adults, this suggests that certain deceptive patterns may continue to be impactful over time due to the long-term financial or privacy implications associated with people's habits around such patterns. For example, when considering Hard to Cancel and Hidden Costs, participants felt strongly against the possibility of being entrapped in recurring subscriptions or unexpected bills without their explicit consent. They conveyed their reluctance to leave unresolved matters for their family to manage, suggesting a deeper awareness of the potential long-term impacts of such designs. Similarly, with Forced Enrolment, participants felt strongly against the sharing of their personal information, sometimes even resorting to the creation of separate email accounts for spam prevention. This aligns with previous research on deceptive patterns, wherein people especially did not excuse the sneaking of additional costs or demands of personal information [33,55]. Older adults seemingly approach deceptive patterns with long-term financial and privacy consequences with heightened sensitivity, suggesting that more work could be done to draw out links between people's degree of prior exposure and their sensitivity to some patterns.

Study 1 further showed that Hidden Costs and Hard to Cancel, which delayed information giving, make older adults more vulnerable and ageing factors such as decreased eyesight made them greater targets. Unlike Van Nimwegen and De Wit's [71] work, which suggested sites that e.g., sneak items into the basket make older adults more cautious, our findings showed that age-related factors do make them more vulnerable and often less cautious. HCI researchers and practitioners working with deceptive patterns must therefore consider educating around vulnerabilities, empowering older adults to navigate online environments confidently and informedly.

Whilst many e-commerce websites operate within a business model that revolves around profit generation, and while it appears that some businesses consider behaviour modification to be a necessary means for survival within the industry, our findings suggest this is not always true. As literature has suggested, prolonged deceptive pattern encounters erode people's trust [7], a trend also supported by Study 1. The erosion of trust carries tangible consequences for businesses, as it often causes people to abandon the website and seek alternatives [7], echoed in Study 1, where a considerable number of participants demonstrated engaging in avoidant behaviours (e.g., clicking away from the site or avoiding it entirely) due to the presence of deceptive patterns. As such, HCI researchers and practitioners should work with companies to demonstrate the far-reaching implications of incorporating deceptive patterns into their designs for older adults, as these practices yield unintended outcomes.

### 6.2 Using Shopopolis to Support Older Adults' E-Commerce Awareness

Study 2 showed that older adults are generally aware of the influence that deceptive patterns can exert on them, even before being actively inoculated. This aligns with past research indicating that older adults are aware of online safety risks, which translates into a cautious approach when interacting with online services, particularly financial ones [27]. However, this contradicts Bongard-Blanchy et al. [8] who concluded that participants aged 40 or above were less likely to be aware of manipulative attempts online. Supporting our findings from Study 1, there was also a significant increase in older adults' awareness of the potential harm of manipulative designs online after playing Shopopolis. Additionally, participants' awareness of the influence of website design on their personal choices online also increased after using Shopopolis. These findings suggest that the *refutational pre-emption* component in Shopopolis was implemented successfully, as inoculated participants were better equipped with relevant information from gameplay to strengthen their negative attitudes towards deceptive patterns compared to uninoculated participants [20]. By using Tetris as a control condition, which is a game like Shopopolis, the study maintained a consistent level of engagement across both groups. This ensured that any changes in awareness or attitudes could be more confidently attributed to the specific content and mechanics of Shopopolis, rather than differences in engagement levels. That said, while our results indicate that reinforcing negative attitudes increased overall awareness of deceptive practices, the subsequent impact on user experiences, such as potentially greater frustration when dealing with difficult cancellation methods, remains to be explored.

Shopopolis also revealed that personal influence did not extend to people's general perspectives after inoculation. One plausible explanation for this discrepancy could be attributed to Shopopolis' approach of educating players from an individual welfare normative lens [58] (that is, viewing deceptive patterns based on whether they diminish individual consumer welfare rather than collective welfare). This emphasis on evaluating deceptive patterns based on their individual impact is important and suggests that whilst collective impact might prompt participants to connect preventative concepts more closely with their personal experiences, individual awareness of personal welfare is most critical to mitigating deceptive patterns' influence.

The individual-centric approach [37,58] resonates particularly strongly within the context of shopping websites, where concerns related to financial loss, cognitive burden, and privacy infringement are commonplace [18]. Previous literature has revealed that the collective dissemination of information [7,48,58,86] significantly impacts societal discourse and behaviour and that it extends beyond e-commerce often onto social media [65,85]. While our study focussed on individual welfare within the context of shopping websites, we recognise the broader implications of deceptive patterns on collective outcomes. There is much potential to explore this dynamic further, considering these contextual intricacies in future research.

Study 2 revealed that playing Shopopolis increased older adults' worries about the danger represented by deceptive patterns from both a personal and general perspective. This finding implies that the *threat* component in Shopopolis was effective in forewarning players of the potential risks of e-commerce deceptive patterns and that older adults worried more for other people than for themselves. This confirms previous assumptions about online risk appraisal, where older adults often consider themselves to be less vulnerable to risks than the general population [95]. This finding extends Study 1 implying that older adults' vulnerability to information hiding deceptive patterns might be exacerbated due to potential age-related factors.

More optimistically, older adults in Study 2 could have possessed a higher level of digital literacy (and therefore a greater understanding of online risks) than the broader user population, given their recruitment through an online survey website. The Control group (not inoculated) reported increased general and personal worries, which might also be attributed to their digital literacy and engagement with the Spot-the-Deceptive-Pattern task prompting them to reflect on deceptive patterns. However, the group lacked the exposure to Shopopolis fully required to understand the mechanics behind these patterns' harmful effects. These findings suggest that when designing future deceptive pattern interventions, designers should not only educate older adults about the existence and impact of deceptive patterns, but also consider varying levels of digital literacy and how information is processed by older adults for their own welfare [56,58].

### 6.3 Supporting Long-Term Recognition of Deceptive Patterns for Older Adults

Our findings revealed that it was also important to consider the impact of long-term exposure to deceptive patterns on older adults' e-commerce habits. Before using Shopopolis, the mean deceptive pattern recognition scores for the Inoculation group and the Control group were 3.78 and 4.24 out of 10, indicating that even without any prior exposure, older adults demonstrated some recognition towards manipulative designs. While our study did not directly compare the recognition scores of younger and older generations, when considering the findings of Bongard-Blanchy et al. [8], which suggested that older people may struggle to identify manipulative attempts, we could infer that older adults' ability to recognise such attempts can vary depending on contextual factors and the specific types of deceptive patterns assessed.

Shopopolis was successful in increasing older adults' recognition abilities of e-commerce deceptive patterns after gameplay and we contribute to broader inoculation research by showing that inoculations of our type have the potential to help bolster resistance to manipulative website designs for older adults. This is in line with prior studies that have demonstrated the efficacy of inoculations in building resilience to misinformation tactics [54,82]. We recommend that ongoing refinements based on user feedback and iterative testing could ensure a more effective and engaging learning process, effectively scaffolding longer-term resilience in older adults to deceptive patterns if they were e.g., exposed to Shopopolis for longer with support provided in-kind, or if the inoculation was expanded to include other types of tasks. For example, HCI researchers could expand on the aforementioned [8] tasks chosen for Shopopolis in this study and investigate other deceptive pattern tasks specific to older adults that could better scaffold their resilience in the long term [82].

## 7 LIMITATIONS AND FUTURE WORK

Recruitment for both studies used online platforms, social media, and crowdsourcing, and sample sizes were relatively small. Therefore, it is likely that participants were more familiar with online designs than less digitally literate older adults. Our findings could thus overestimate what the less technologically literate older adult population is aware of regarding e-commerce deceptive patterns. Moreover, since recruitment was not limited by country of residence, this raises the possibility of divergent conclusions based on cultural differences or location-specific effects [39]. It should be further mentioned that older adults' awareness of and concern about the influence of manipulative design stemmed from a self-reported measure. Bongard-Blanchy et al. [8] also caution that this does not necessarily reflect actual behaviour, which introduces approximation into the measure.

Study 2 examined the immediate effects of inoculation through Shopopolis gameplay. As such, the long-term impact of Shopopolis on older adults' resistance to deceptive patterns remains largely unexplored. Given that past research in the misinformation domain has shown that inoculation effects can remain stable for at least three months [54], we believe there is potential that the inoculation effect on manipulative designs could exhibit similar longevity. Future research could aim to address this limitation by conducting follow-up assessments over an extended timeframe, enabling a longitudinal evaluation of the intervention's effects.

It is also important to consider other implications of Shopopolis' design. The current win-state, similar to Roozenbeek and van der Linden's "Bad News" game [83], involves putting the player in the shoes of the manipulator and encouraging use of more deceptive patterns to increase sales. This design facilitates inoculation compared to a win-state where no deceptive patterns are incentivised, as it provides players with first-hand experience of manipulative tactics, fostering critical assessment. Without the incentive to use deceptive patterns, players might not fully explore or understand the intricacies of these tactics, limiting their exposure and learning opportunities. However, this approach might unintentionally reinforce the notion that deceptive patterns are necessary for success in e-commerce, especially if players do not fully engage with the game's reflections (e.g., ethical implications). Furthermore, players who do not fully engage with the reflective prompts might miss the critical assessment component, leading to a less effective inoculation against these tactics. While this seems unlikely given our older adult participants showed an attitudinal change (increased awareness and concern) about deceptive patterns post-inoculation, it is crucial to consider these outcomes when adapting the game for different and potentially more impressionable audiences in future iterations.

Finally, while Shopopolis was designed with the lived experiences of older adults in mind, its gamified approach has the potential to raise awareness of deceptive patterns among various populations, particularly those with limited technology exposure. That said, because end users' technology goals and usage contexts are dynamic and individualised, there is no one-size-fits-all solution to combatting deceptive patterns. Similar to the approach taken in this research, tailoring the game to the needs and perceptions of the population of interest is crucial. This might involve shaping the game's content to focus on deceptive patterns that are most impactful for this population and situating these patterns within scenarios they most commonly encounter (e.g., during online purchases, account registrations, or promotional offers). Future research would benefit from exploring the adaptability and effectiveness of gamified inoculation interventions like Shopopolis across user groups and web service contexts. Moreover, investigating how inoculation games can complement other interventions to support critical thinking [49], evaluations of online information [74], and unintended consumption [45] would be valuable. This holistic approach could contribute to fully mitigating the impact of deceptive patterns.

## 8 CONCLUSION

Deceptive patterns pose an increasing threat to the online environment. This research demonstrates a need to understand the unique ways in which older adults engage with e-commerce services, and how these approaches shape their interactions with various types of deceptive patterns. Our findings highlight the role of age-related factors in moulding their responses to manipulative designs, indicating the necessity of tailored interventions, and how gamified inoculation, exemplified by Shopopolis, holds promise as a means to enhance older adults' awareness, concern, and recognition of deceptive patterns. Our approach seeks to empower older adults to resist manipulative designs but also underscores the importance of

engaging with educational tools to fostering digital literacy within this demographic. We also advocate those inside and outside of HCI, including designers, researchers, practitioners, policymakers, and educators, to consider older adults' inoculation preferences to help create safer digital environments for them.

## ACKNOWLEDGEMENTS

The authors would like to thank the participants for their time and engagement with this research project. This project was funded through the EPSRC Equity for the Older: Beyond Digital Access (EP/W025337/1) grant.

## A STUDY 1: ONLINE SURVEY

Following demographic questions about age and gender, participants were asked to read this passage carefully before continuing the survey:

- Deceptive patterns are design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that they otherwise would not make if fully informed and capable of selecting alternatives. Such deceptive patterns are becoming increasingly ubiquitous, especially on online shopping websites. Although deceptive patterns affect users of all ages, older adults are currently an understudied demographic in this context. The following questions will probe into your previous experiences, if any, with deceptive patterns within e-commerce. You will be presented with 7 deceptive patterns found on shopping websites and asked if you have personally encountered each deceptive pattern before, what you thought of it at the time, and how it made you feel or behave.

Participants were then presented with examples of seven deceptive patterns from Mathur et al.'s [59] taxonomy:

- *Deceptive Pattern 1 of 7: Hidden Costs.* For example, a hotel might advertise a room for $100 per night, but then add a $50 "resort fee" at checkout that was not clearly disclosed earlier.
- *Deceptive Pattern 2 of 7: Deceptive Countdown Timers.* For example, an advertised offer of "2 shirts for $19.99" remains valid even after the countdown timer expires.
- *Deceptive Pattern 3 of 7: Confirmshaming.* For example, a website using language like "No thanks, I don't want to save money" on a pop-up that encourages users to sign up for a newsletter or make a purchase.
- *Deceptive Pattern 4 of 7: Activity Notifications.* For example, a website using dynamic and periodic messages to indicate how many users have a specific item in their cart (e.g., "35 people added this item to cart").
- *Deceptive Pattern 5 of 7: High-demand Messages.* For example, messages indicating that the products in the cart are selling out quickly (e.g., "Items in your cart are in high demand").
- *Deceptive Pattern 6 of 7: Hard to Cancel.* For example, making it easy for users to sign up for recurring subscriptions, but hard for them to subsequently cancel the subscriptions (e.g., by requiring them to call customer service).

- *Deceptive Pattern 7 of 7: Forced Enrolment.* For example, preventing users from viewing product offerings on the website without creating an account—even if users eventually decide against making a purchase.

After presentation of each pattern, participants were asked the following questions:

- Have you ever encountered this deceptive pattern on an e-commerce or shopping website before? (Yes/No)
- How did it make you feel? Select all that apply. (Annoyed/Concerned/Angry/Stressed/None of the above/Other)
- At the time, did you realise that the website was employing a deceptive design choice? If you knew, would you behave differently?
- Optional question: If you can remember, what shopping website(s) did you encounter it on?
- Optional question: What might help you to spot this deceptive pattern in the future?

These questions were asked to gain more insight into participants' perspectives towards the seven deceptive patterns:

- Which deceptive pattern(s) do you believe is the most concerning and therefore the most important ***for you*** to identify when shopping online? Please select as many options as you like.
- Why have you chosen this deceptive pattern(s) as most concerning and important to identify?
- How often do you encounter deceptive patterns when using shopping websites? (Always/Often/Sometimes/Rarely/Never)
- Were you familiar with the concept of deceptive patterns before taking this survey? (Yes/No)

Finally, participants were asked questions related to their gaming experiences. Multiple choice options were formulated based on past research:

- Have you ever played a video game before/do you play video games? (Yes/No)
- As an older adult, do you face any of these challenges when playing existing video games? Select all that apply. (Video games can be difficult to learn/Video games can be difficult to play or operate/Video game controls can be difficult to remember/Playing video games takes up too much time/Video games cause too much frustration/None of the above/Other).
- If a video game was created to help older adults identify different deceptive patterns on shopping websites, what features would be most important to include? Select all that apply. (It should be an educational-based game about deceptive patterns/It should be a puzzle and strategy-based game about deceptive patterns/It should be an awareness-based game about deceptive patterns/It should be an action and adventure-based game about deceptive patterns/Other).

## B STUDY 1: CODEBOOK

| Initial Code | Definition | Example Text |
|---|---|---|

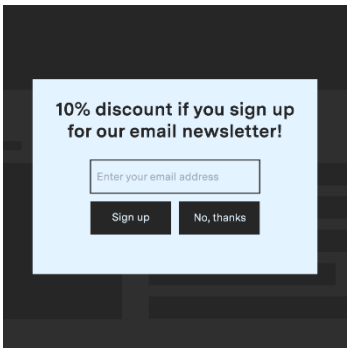
| | | |
|---|---|---|
| Hard to Cancel Frustration | Instances where participants expressed frustration due to difficulty in cancelling a service. | "It would take half a lifetime to cancel/discontinue" (P50) |
| Hidden Costs Confusion | Instances where participants were confused by additional costs revealed late in the purchase process. | "I thought it helped to show me where to click!" (P28) |
| Avoidant Behaviour | Instances where participants avoided certain websites or services due to deceptive practices. | "If I know it will be hard to cancel, I won't sign up." (P45) |
| Awareness of Manipulative Intent | Instances where participants recognised manipulative design choices. | "I knew it was manipulation." (P18) |
| Reading Fine Print | Instances where participants mentioned the importance of reading fine print to avoid deception. | "I just read the fine print" (P12) |
| Forced Enrolment Annoyance | Frustration with being forced to create an account to access content. | "I just click away and Google the story." (P9) |
| Activity Notifications Skepticism | Doubt about the authenticity of activity notifications. | "I look at the numbers and decide if they have any truth. If it's unlikely I pass." (P44) |
| Cost Comparison | Actions taken to compare costs across platforms to avoid hidden fees. | "I don't shop just one site. This means when I cost comparison I need to get competitor sites to the check out point to make a decision. I also make use of 3rd party shopping tools that show the total price." (P42) |
| Preference for Transparency | Preference for clear and honest communication from websites. | "I would prefer that they would be honest about it or provide clarity" (P49) |
| Limited Trust | Reduced trust in certain platforms due to repeated deceptive practices. | "I don't respond well to this tactic and usually stick to a handful of trusted sites for shopping, news subscription services and financial sites." (P13) |
| Adaptive Coping | Strategies used by participants to mitigate the effects of deceptive patterns. | "I use a dedicated 'spam' email address for sign-ups to avoid spam." (P42) |
| Caution Due to Long-term Impact | Increased caution toward long-term effects of deceptive patterns, especially among older adults. | "I don't want to leave subscriptions for others to end." (P16) |
| Discount Seeking | Waiting for discounts despite deceptive urgency tactics like countdown timers. | "Yes, I would do what I did and place the item in the shopping cart and waited several days until they sent me a 20% off code." (P48) |
| Seeking Reviews and Recommendations | Seeking advice or checking reviews from others to avoid deceptive websites. | "I try and read reviews before I shop at a website I am unfamiliar with." (P25) |
| Reporting Deceptive Practices | Reporting deceptive practices to consumer protection agencies or warning others through negative reviews. | "I stopped right here, and gave it a negative review over this charge." (P9) |

Table 4. Codebook of initial codes after the first round of open coding.

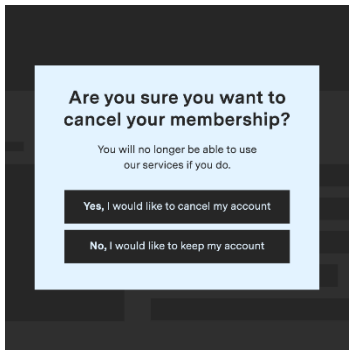
| Higher-Level Code | Definition | Example Initial Code |
|---|---|---|
| Trust Erosion | Instances where deceptive practices led to a loss of trust towards the website or service. | Hard to Cancel Frustration, Hidden Costs Confusion, Limited Trust, Reporting Deceptive Practices |
| Emotional Response | Emotional reactions to deceptive practices, such as frustration, anger, or stress. | Hard to Cancel Frustration, Awareness of Manipulative Intent, Forced Enrolment Annoyance |
| Behavioural Response | Changes in behavior as a result of encountering deceptive practices. | Avoidant Behaviour, Reading Fine Print, Cost Comparison, Seeking Reviews and Recommendations, Reporting Deceptive Practices |
| Desire for Autonomy | Instances where participants expressed a desire for more control and transparency in their interactions. | Awareness of Manipulative Intent, Preference for Transparency, Forced Enrolment Annoyance |
| Cost-Related Tolerance | Instances where participants indicated a threshold for acceptable additional costs. | Hidden Costs Confusion, Reading Fine Print, Cost Comparison, Discount Seeking |
| Knowledge and Recognition | Understanding and identifying deceptive patterns. | Awareness of Manipulative Intent, Activity Notifications Skepticism, Seeking Reviews and Recommendations |
| Adaptive Strategies | Methods used by participants to mitigate the impact of deceptive patterns. | Adaptive Coping, Caution Due to Long-term Impact, Discount Seeking |

Table 5. Mapping of initial codes to their corresponding higher-level codes.

## C STUDY 2: SPOT-THE-DECEPTIVE-PATTERN (STDP) TASK INTERFACES

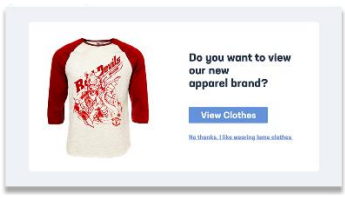



(a) Control

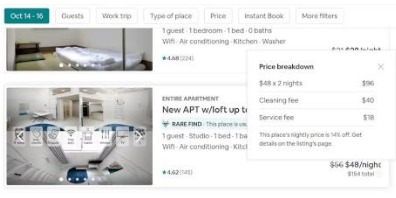



(b) Control

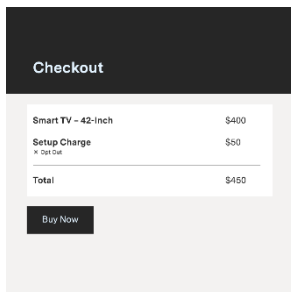

(c) Misdirection



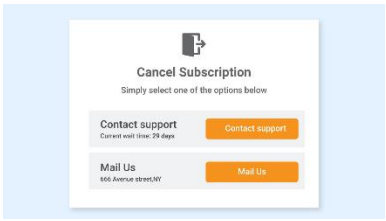

(d) Misdirection



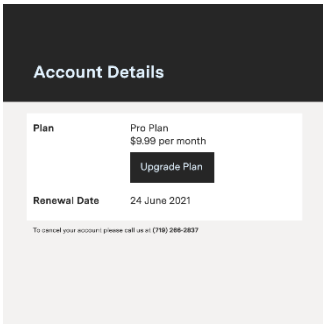

(e) Sneaking




(f) Sneaking

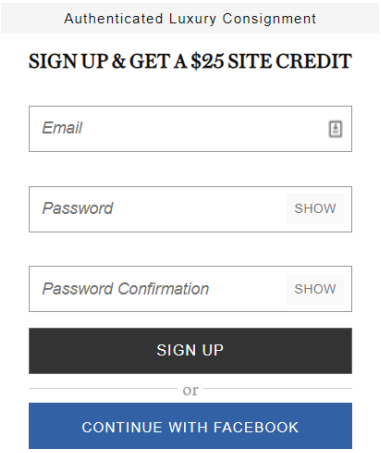



(g) Obstruction




(h) Obstruction


(i) Forced Action




(j) Forced Action

## REFERENCES

[1] Jacob Aagaard, Miria Emma Clausen Knudsen, Per Bækgaard, and Kevin Doherty. A Game of Dark Patterns: Designing Healthy, Highly-Engaging Mobile Games. In CHI Conference on Human Factors in Computing Systems Extended Abstracts, ACM, 1–8. https://doi.org/10.1145/3491101.3519837

[2] Reza Ghaiumy Anaraky, Kaileigh Angela Byrne, Pamela J. Wisniewski, Xinru Page, and Bart Knijnenburg. To Disclose or Not to Disclose: Examining the Privacy Decision-Making Processes of Older vs. Younger Adults. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, 1–14. https://doi.org/10.1145/3411764.3445204

[3] Simone Avolicino, Marianna Gregorio, Fabio Palomba, Marco Romano, Monica Sebillo, and Giuliana Vitiello. AI-Based Emotion Recognition to Study Users' Perception of Dark Patterns. 185–203. https://doi.org/10.1007/978-3-031-17615-9_13

[4] John A. Banas and Stephen A. Rains. A Meta-Analysis of Research on Inoculation Theory. Commun Monogr 77, 3, 281–311. https://doi.org/10.1080/03637751003758193

[5] Melisa Basol, Jon Roozenbeek, Manon Berriche, Fatih Uenal, William P. McClanahan, and Sander Linden. Towards psychological herd immunity: Cross-cultural evidence for two prebunking interventions against COVID-19 misinformation. Big Data Soc 8, 1, 205395172110138. https://doi.org/10.1177/20539517211013868

[6] Melisa Basol, Jon Roozenbeek, and Sander Linden. Good News about Bad News: Gamified Inoculation Boosts Confidence and Cognitive Immunity Against Fake News. J Cogn 3, 1, 2. https://doi.org/10.5334/joc.91

[7] Aditi M. Bhoot, Mayuri A. Shinde, and Wricha P. Mishra. Towards the Identification of Dark Patterns: An Analysis Based on End-User Reactions. In IndiaHCI '20: Proceedings of the 11th Indian Conference on Human-Computer Interaction, ACM, 24–33. https://doi.org/10.1145/3429290.3429293

[8] Kerstin Bongard-Blanchy, Arianna Rossi, Salvador Rivas, Sophie Doublet, Vincent Koenig, and Gabriele Lenzini. I am Definitely Manipulated, Even When I am Aware of it. It's Ridiculous!" - Dark Patterns from the End-User Perspective. In Designing Interactive Systems Conference 2021, ACM, 763– 776. https://doi.org/10.1145/3461778.3462086

[9] Ida Marie Borberg, Rene Hougaard, Willard Rafnsson, and Oksana Kulyk. "So I Sold My Soul": Effects of Dark Patterns in Cookie Notices on End- User Behavior and Perceptions. In Proceedings 2022 Symposium on Usable Security, Internet Society. https://doi.org/10.14722/usec.2022.23026

[10] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. In Proceedings on Privacy Enhancing Technologies 2016, 237–254. . https://doi.org/10.1515/popets-2016-0038

[11] David M. Boush, Marian Friestad, and Peter Wright. 2015. Deception In The Marketplace. Routledge. https://doi.org/10.4324/9780203805527

[12] Elizabeth A. Boyle, Thomas Hainey, Thomas M. Connolly, Grant Gray, Jeffrey Earp, Michela Ott, Theodore Lim, Manuel Ninaus, Claudia Ribeiro, and João Pereira. An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. Comput Educ 94, 178–192. https://doi.org/10.1016/j.compedu.2015.11.003

[13] Petter Bae Brandtzæg, Marika Lüders, and Jan Håvard Skjetne. Too Many Facebook "Friends"? Content Sharing and Sociability Ver sus the Need for Privacy in Social Network Sites. Int J Hum Comput Interact 26, 11–12. https://doi.org/10.1080/10447318.2010.516719

[14] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. Qual Res Psychol 3, 2, 77–101. https://doi.org/10.1191/1478088706qp063oa

[15] Harry Brignull. Dark patterns: inside the interfaces designed to trick you. Retrieved from https://www.theverge.com/2013/8/29/4640308/dark-patterns

[16] Harry Brignull, Mark Leiser, Cristiana Santos, and Kosha Doshi. Deceptive patterns – user interfaces designed to trick you. deceptive.design.

[17] Evert Broeck, Karolien Poels, and Michel Walrave. Older and Wiser? Facebook Use, Privacy Concern, and Privacy Protection in the Life Stages of Emerging, Young, and Middle Adulthood. Soc Media Soc 1, 2, 205630511561614. https://doi.org/10.1177/2056305115616149

[18] Deon Soul Calawen. Dark Patterns: Effect on Overall User Experience and Site Revisitation. Technological University Dublin.

[19] Joshua A. Compton. Inoculation theory. In The SAGE handbook of persuasion: Developments in theory and practice. Sage Publications, Inc, 220– 236.

[20] Joshua A. Compton and Michael Pfau. Inoculation Theory of Resistance to Influence at Maturity: Recent Progress In Theory Deve lopment and Application and Suggestions for Future Research. Ann Int Commun Assoc 29, 1, 97–146. https://doi.org/10.1080/23808985.2005.11679045

[21] Thomas M. Connolly, Elizabeth A. Boyle, Ewan MacArthur, Thomas Hainey, and James M. Boyle. A systematic literature review of empirical evidence on computer games and serious games. Comput Educ 59, 2, 661–686. https://doi.org/10.1016/j.compedu.2012.03.004

[22] Lorrie Faith Cranor. Cookie monster. Commun ACM 65, 7, 30–32. https://doi.org/10.1145/3538639

[23] Johan Creutzfeldt, Leif Hedman, and Li Felländer-Tsai. Effects of pre-training using serious game technology on CPR performance – an exploratory quasi-experimental transfer study. Scand J Trauma Resusc Emerg Med 20, 1, 79. https://doi.org/10.1186/1757-7241-20-79

[24] Gregory Day and Abbey Stemler. Are Dark Patterns Anticompetitive? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3468321

[25] Natalie C. Ebner, Donovan M. Ellis, Tian Lin, Harold A. Rocha, Huizi Yang, Sandeep Dommaraju, Adam Soliman, Damon L. Woodard, Gary R. Turner, R. Nathan Spreng, and Daniela S. Oliveira. 2020. Uncovering Susceptibility Risk to Online Deception in Aging. The Journals of Gerontology: Series B 75, 3 (February 2020), 522–533. https://doi.org/10.1093/geronb/gby036

[26] Ullrich K. H. Ecker, Stephan Lewandowsky, John Cook, Philipp Schmid, Lisa K. Fazio, Nadia Brashier, Panayiota Kendeou, Emily K. Vraga, and Michelle A. Amazeen. The psychological drivers of misinformation belief and its resistance to correction. Nature Reviews Psychology 1, 1, 13–29. https://doi.org/10.1038/s44159-021-00006-y

[27] Dandi Feng, Hiba Rafih, and Cosmin Munteanu. Understanding Older Adults' Safety Perceptions and Risk Mitigation Strategies when Accessing Online Services. 467–491. https://doi.org/10.1007/978-3-031-35822-7_31

[28] Linda Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. UI Dark Patterns and Where to Find Them. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, 1–14. . https://doi.org/10.1145/3313831.3376600

[29] Lorna Gibson, Wendy Moncur, Paula Forbes, John Arnott, Christopher Martin, and Amritpal S. Bhachu. Designing Social Networking Sites for Older Adults. https://doi.org/10.14236/ewic/HCI2010.24

[30] Leo A. Goodman. Snowball Sampling. The Annals of Mathematical Statistics 32, 1, 148–170.

[31] Chad Phoenix Rose Gowler, Ioanna Iacovides, and Leo A. Goodman. "Horror, guilt and shame" – Uncomfortable Experiences in Digital Games. In Proceedings of the Annual Symposium on Computer-Human Interaction in Play, ACM, 325–337. . https://doi.org/10.1145/3311350.3347179

[32] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius, and Moniek Buijzen. Dark and Bright Patterns in Cookie Consent Requests. Journal of Digital Social Research 3, 1, 1–38. https://doi.org/10.33621/jdsr.v3i1.54

[33] Colin M. Gray, Jingle Chen, Shruthi Sai Chivukula, and Liyang Qu. End User Accounts of Dark Patterns as Felt Manipulation. Proc ACM Hum Comput Interact 5, CSCW2, 1–25. https://doi.org/10.1145/3479516
[34] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, 1–14. . https://doi.org/10.1145/3173574.3174108
[35] Galen A. Grimes, Michelle G. Hough, and Margaret L. Signorella. Email end users and spam: relations of gender and age group to attitudes and actions. Comput Human Behav 23, 1, 318–332. https://doi.org/10.1016/j.chb.2004.10.015
[36] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. Proc ACM Hum Comput Interact 5, CSCW2, 1–29. https://doi.org/10.1145/3479521
[37] Johanna Gunawan, Cristiana Santos, and Irene Kamara. Redress for Dark Patterns Privacy Harms? A Case Study on Consent Interac tions. In Proceedings of the 2022 Symposium on Computer Science and Law, ACM, 181–194. . https://doi.org/10.1145/3511265.3550448
[38] A. J. Haywood. Online Auctions: User Experience Insights from eBay.
[39] Shun Hidaka, Sota Kobuki, Mizuki Watanabe, and Katie Seaborn. Linguistic Dead-Ends and Alphabet Soup: Finding Dark Patterns in Japanese Apps. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, ACM, 1–13. https://doi.org/10.1145/3544548.3580942
[40] Soheil Human and Florian Cech. A Human-Centric Perspective on Digital Consenting: The Case of GAFAM. 139–159. https://doi.org/10.1007/978-981-15-5784-2_12
[41] Jae Min Jung and James J. Kellaris. Cross-national differences in proneness to scarcity effects: The moderating roles of familiarity, uncertainty avoidance, and need for cognitive closure. Psychol Mark 21, 9, 739–753. https://doi.org/10.1002/mar.20027
[42] Lexie Kane. The Attention Economy. Retrieved from https://www.nngroup.com/articles/attention-economy/.
[43] Woo Gon Kim, Souji Gopalakrishna Pillai, Kavitha Haldorai, and Wasim Ahmad. Dark patterns used by online travel agency websites. Ann Tour Res 88, 103055. https://doi.org/10.1016/j.annals.2020.103055
[44] Bran Knowles and Vicki L. Hanson. The wisdom of older technology (non)users. Commun ACM 61, 3, 72–77. https://doi.org/10.1145/3179995
[45] Woon Chee Koh and Yuan Zhi Seah. Unintended consumption: The effects of four e-commerce dark patterns. Cleaner and Responsible Consumption 11, 100145. https://doi.org/10.1016/j.clrc.2023.100145
[46] Konrad Kollnig, Siddhartha Datta, and Max Kleek. I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, 1–8. https://doi.org/10.1145/3411763.3451632
[47] Dr Mark Leiser. "Dark Patterns": The Case for Regulatory Pluralism. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3625637
[48] Jamie Luguri and Lior Jacob Strahilevitz. Shining a Light on Dark Patterns. Journal of Legal Analysis 13, 1, 43–109. https://doi.org/10.1093/jla/laaa006
[49] Lauren Lutzke, Caitlin Drummond, Paul Slovic, and Joseph Árvai. 2019. Priming critical thinking: Simple interventions limit the influence of fake news about climate change on Facebook. Global Environmental Change 58, (September 2019), 101964. https://doi.org/10.1016/j.gloenvcha.2019.101964
[50] Ulrik Lyngs, Kai Lukoff, Petr Slovak, William Seymour, Helena Webb, Marina Jirotka, Jun Zhao, Max Kleek, and Nigel Shadbolt. "I Just Want to Hack Myself to Not Get Distracted": Evaluating Design Interventions for Self-Control on Facebook. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, 1–15. https://doi.org/10.1145/3313831.3376672
[51] Michael Lynn. Scarcity effects on value: A quantitative review of the commodity theory literature. Psychol Mark 8, 1, 43–57.
[52] ACM Association for Computing Machinery. Words matter: Alternatives for charged terminology in the computing profession. Retrieved from https://www.acm.org/diversity-inclusion/words-matter.
[53] Dominique Machuletz and Rainer Böhme. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. In Proceedings on Privacy Enhancing Technologies 2020, 481–498. . https://doi.org/10.2478/popets-2020-0037
[54] Rakoen Maertens, Jon Roozenbeek, Melisa Basol, and Sander Linden. Long-term effectiveness of inoculation against misinformation: Three longitudinal experiments. J Exp Psychol Appl 27, 1, 1–16. https://doi.org/10.1037/xap0000315
[55] Maximilian Maier and Rikard Harr. Dark Design Patterns: An End-User Perspective. Human Technology 16, 2, 170–199. https://doi.org/10.17011/ht/urn.202008245641
[56] Ittay Mannheim, Ella Schwartz, Wanyu Xi, Sandra C. Buttigieg, Mary McDonnell-Naughton, Eveline J. M. Wouters, and Yvonne Zaalen. Inclusion of Older Adults in the Research and Design of Digital Technology. Int J Environ Res Public Health 16, 19, 3718. https://doi.org/10.3390/ijerph16193718

[57] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Eli Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. Dark Patterns at Scale. Proc ACM Hum Comput Interact 3, 1–32. https://doi.org/10.1145/3359183

[58] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. What Makes a Dark Pattern... Dark? In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, May 06, 2021. ACM, 1–18. https://doi.org/10.1145/3411764.3445610

[59] William J. McGuire. Some Contemporary Approaches. 191–229. https://doi.org/10.1016/S0065-2601(08)60052-0

[60] William J. McGuire. The Effectiveness of Supportive and Refutational Defenses in Immunizing and Restoring Beliefs Against Persuasion. Sociometry 24, 2, 184. https://doi.org/10.2307/2786067

[61] William J. McGuire. Resistance to persuasion conferred by active and passive prior refutation of the same and alternative counterarguments. The Journal of Abnormal and Social Psychology 63, 2, 326–332. https://doi.org/10.1037/h0048344

[62] William J. McGuire and D. Papageorgis. The relative efficacy of various types of prior belief-defense in producing immunity against persuasion. The Journal of Abnormal and Social Psychology 62, 2, 327–337. https://doi.org/10.1037/h0042026

[63] Tamir Mendel, Roei Schuster, Eran Tromer, and Eran Toch. Toward Proactive Support for Older Adults. Proc ACM Interact Mob Wearable Ubiquitous Technol 6, 1, 1–25. https://doi.org/10.1145/3517249

[64] Christian Meske and Ireti Amojo. Ethical Guidelines for the Construction of Digital Nudges. In 53rd Hawaii International Conference on Systems Sciences (HICSS, 3928–3937).

[65] Thomas Mildner and Gian-Luca Savino. Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, ACM, 1–7. https://doi.org/10.1145/3411763.3451659

[66] Thomas Mildner, Gian-Luca Savino, Philip R. Doyle, Benjamin R. Cowan, and Rainer Malaka. About Engaging and Governing Strategies: A Thematic Analysis of Dark Patterns in Social Networking Services. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, ACM, 1–15. https://doi.org/10.1145/3544548.3580695

[67] Luigi Mittone and Lucia Savadori. The Scarcity Bias. Applied Psychology 58, 3, 453–468. https://doi.org/10.1111/j.1464-0597.2009.00401.x

[68] Carol Moser. Impulse Buying: Designing for Self-Control with E-commerce. University of Michigan.

[69] Carol Moser, Sarita Y. Schoenebeck, and Paul Resnick. Impulse Buying: Design Practices and Consumer Needs. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 02, 2019. ACM, 1–15. https://doi.org/10.1145/3290605.3300472

[70] James Nicholson, Lynne Coventry, and Pam Briggs. Age-related performance issues for PIN and face-based authentication systems. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 323–332. https://doi.org/10.1145/2470654.2470701

[71] Christof van Nimwegen and Jesse de Wit. 2022. Shopping in the Dark. 462–475. https://doi.org/10.1007/978-3-031-05412-9_32

[72] Chris Nodder. Evil by design: Interaction design to lead us into temptation. John Wiley & Sons.

[73] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, 1–13. https://doi.org/10.1145/3313831.3376321

[74] Thomas Nygren, Fredrik Brounéus, and Göran Svensson. 2019. Diversity and Credibility in Young People's News Feeds: A Foundation for Teaching and Learning Citizenship in a Digital Era. JSSE - Journal of Social Science Education (March 2019), Vol 18 No 2 (2019). https://doi.org/10.4119/JSSE-917

[75] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. Turtle s, locks, and bathrooms: Understanding mental models of privacy through illustration. In Proceedings on Privacy Enhancing Technologies 2018, 5–32.

[76] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting Spear Phishing Emails for Older vs Young Adults. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, ACM, 6412–6424. https://doi.org/10.1145/3025453.3025831

[77] Stefan Palan and Christian Schitter. Prolific.ac—A subject pool for online experiments. J Behav Exp Finance 17, 22–27. https://doi.org/10.1016/j.jbef.2017.12.004

[78] Anabel Quan-Haase and Isioma Elueze. Revisiting the Privacy Paradox. In Proceedings of the 9th International Conference on Social Media and Society, ACM, 150–159. https://doi.org/10.1145/3217804.3217907

[79] Hirak Ray, Flynn Wolf, Ravi Kuber, and Adam J. Aviv. "Woe is me": Examining Older Adults' Perceptions of Privacy. In Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems, ACM, 1–6. https://doi.org/10.1145/3290607.3312770

[80] Ute Ritterfeld, Cuihua Shen, Hua Wang, Luciano Nocera, and Wee Ling Wong. Multimodality and Interactivity: Connecting Properties of Serious Games with Educational Outcomes. CyberPsychology & Behavior 12, 6, 691–697. https://doi.org/10.1089/cpb.2009.0099

[81] Alberto Monge Roffarello and Luigi Russis. Towards Understanding the Dark Patterns That Steal Our Attention. In CHI Conference on Human Factors in Computing Systems Extended Abstracts, ACM, 1–7. https://doi.org/10.1145/3491101.3519829

[82] Jon Roozenbeek and Sander Linden. The fake news game: actively inoculating against the risk of misinformation. J Risk Res 22, 5, 570–580. https://doi.org/10.1080/13669877.2018.1443491

[83] Jon Roozenbeek and Sander Linden. Fake news game confers psychological resistance against online misinformation. Palgrave Commun 5, 1, 65. https://doi.org/10.1057/s41599-019-0279-9

[84] Jon Roozenbeek and Sander Linden. Breaking Harmony Square: A game that "inoculates" against political misinformation. Harvard Kennedy School Misinformation Review. https://doi.org/10.37016/mr-2020-47

[85] Brennan Schaffner, Neha A. Lingareddy, and Marshini Chetty. Understanding Account Deletion and Relevant Dark Patterns on Social Media. Proc ACM Hum Comput Interact 6, CSCW2, 1–43. https://doi.org/10.1145/3555142

[86] Simon Shaw. Consumers Are Becoming Wise to Your Nudge. Retrieved from https://behavioralscientist.org/consumers-are-becoming-wise-to- your-nudge/.

[87] Muzafer Sherif. The psychology of social norms.

[88] Ray Sin, Ted Harris, Simon Nilsson, and Talia Beck. Dark patterns in online shopping: do they work and can nudges help mitiga te impulse buying? Behavioural Public Policy, 1–27. https://doi.org/10.1017/bpp.2022.11

[89] Caroline Sinders. 2022. What's In a Name? https://medium.com/@carolinesinders/whats-in-a-name-unpacking-dark-patterns- versusdeceptive-design-e96068627ec4.

[90] Samuel J. Stratton. Population Research: Convenience Sampling Strategies. Prehosp Disaster Med 36, 4, 373–374. https://doi.org/10.1017/S1049023X21000649

[91] The UN Refugee Agency. 2020. Older persons. Retrieved from https://emergency.unhcr.org/protection/persons-risk/older-persons#:~:text=An%20older%20person%20is%20defined,or%20age%2Drelated%20health%20conditions.

[92] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)informed Consent. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, November 06, 2019. ACM, 973–990. https://doi.org/10.1145/3319535.3354212

[93] John Vines, Gary Pritchard, Peter Wright, Patrick Olivier, and Katie Brittain. An Age-Old Problem: Examining the Discourses of Ageing in HCI and Strategies for Future Research. ACM Transactions on Computer-Human Interaction 22, 1, 1–27. https://doi.org/10.1145/2696867

[94] Kerryellen G. Vroman, Sajay Arthanat, and Catherine Lysack. "Who over 65 is online?" Older adults' dispositions toward information communication technology. Comput Human Behav 43, 156–166. https://doi.org/10.1016/j.chb.2014.10.018

[95] Ryan West. The psychology of security. Commun ACM 51, 4, 34–40. https://doi.org/10.1145/1330311.1330320

[96] Matthew Alexander Whitby, Sebastian Deterding, and Ioanna Iacovides. "One of the baddies all along": Moments that Challenge a Player's Perspective. In Proceedings of the Annual Symposium on Computer-Human Interaction in Play, ACM, 339–350. https://doi.org/10.1145/3311350.3347192

[97] Pieter Wouters, Christof Nimwegen, Herre Oostendorp, and Erik D. Spek. A meta-analysis of the cognitive and motivational effects of serious games. J Educ Psychol 105, 2, 249–265. https://doi.org/10.1037/a0031311

[98] José P. Zagal, Staffan Björk, and Chris Lewis. Dark patterns in the design of games. Foundations of Digital Games.

Received February 2024; revised June 2024; accepted July 2024.