Security Journal (2025) 38:49
https://doi.org/10.1057/s41284-025-00487-z

S.I.: PREVENTING FRAUD AND CYBERCRIME IN AN AGEING SOCIETY AND POTENTIAL

The wisdom of the scammed: redefining older fraud victim support by utilizing the ecological systems framework

Katalin Parti[1] · **Faika Tahir**[1] · **Pamela B. Teaster**[2]

Accepted: 16 September 2024

Abstract

Cyber victimization targeting vulnerable populations, particularly older adults, has become increasingly prevalent in the digital age. Grounded in the Bioecological Systems Framework (Bronfenbrenner in The ecology of human development: Experiments by nature and design, Harvard University Press, Cambridge, 1979), this research explores the factors contributing to victimization, including the ease of exploitation, the situational factors setting up victims for scams, their vulnerabilities, the dynamics within their environments, and the challenges victims face in recognizing scams. Using semi-structured interviews, we asked scam victims ($n = 19$) aged 60 years and above about their personal and structural circumstances as well as their individual assessment of the impact of their being victimized. Despite high levels of education and computer literacy among our sample, their victimization occurred far too frequently, which prompts a call for the revision of existing approaches toward helping older adults overcome scam victimization.

Keywords Scam · Fraud · Victimization · Older adults · Ecological systems theory · Policy

Introduction

Online fraud victimization can be defined as the suffering of a loss, financial or otherwise, or of any other impact due to an individual providing personal information or money via the internet in response to a dishonest invitation, request, notification, or offer (Cross et al. 2014). In addition, this manuscript conceptualizes fraud as scams committed by strangers, and as such, family members, caretakers, and other trusted

✉ Katalin Parti
kparti@vt.edu

[1] Department of Sociology, Virginia Tech, Blacksburg, VA, USA

[2] Center for Gerontology, Virginia Tech, Blacksburg, VA, USA

Published online: 25 June 2025

individuals are not part of the offender group. Cyber victimization targeting vulnerable populations, particularly older adults, has become increasingly prevalent in the digital age. In 2022, the FBI received 800,944 complaints, with reported losses exceeding $10.3 billion (IC3 2023). Over 88,000 fraud victims were identified as being over 60, resulting in approximately $3.1 billion in losses to older Americans. This represents an increase of approximately $1.4 billion in losses reported by this group in 2022 versus in 2021 (IC3 2023).

Older adults tend to experience lower rates of victimization for crimes in general compared to younger adults. However, older adults are more susceptible to certain types of crimes, particularly scams and financial fraud (Button et al. 2024a). The National Institute of Justice highlights that those aged 60 years and above are frequently targeted by financial fraud schemes (Morgan and Tapp 2024). In 2017, about 1.33% of older adults experienced at least one incident of financial fraud, which includes scams related to products and services, phantom debt, and prize or grant frauds. This rate was not significantly higher than for younger adults, but the nature of the scams often exploited the vulnerabilities associated with aging, such as cognitive decline and social isolation (Morgan and Tapp 2024). Although we do not know how many Americans are victimized by scams due to underreporting (Ianzito 2024; Cross et al. 2018), studies corroborate older age groups' relatively high vulnerability to scams. For example, the 2016 Health and Retirement Study found that 34.8% of persons aged 50 years or older had been targeted by or had been the victim of a fraud or investment scam in the past 5 years (DeLiema et al. 2020). This indicates a relatively higher rate of scam victimization in older age groups. In addition, while older people are still less likely to become scam victims, they lose more money to scams than their younger counterparts (Button et al. 2024a; Federal Trade Commission 2024).

Older age groups' relative high vulnerability to scams lies in various individual, social, and economic factors. As such, online communication has been increasing independent of age, but is has been especially dramatic in individuals 65 and older (Faviero 2022) which put older age groups at risk of scam victimization. Another risk factor is that older adults have 71% of the total wealth share in the US economy, meaning they represent a generation with much to lose financially (Vandenbroucke and Zhu 2017), making them a lucrative target. Besides, older adults' trusting nature (Robinson and Edwards 2024), compassion (Coombs 2014), shaped by social norms of politeness, makes them less suspicious of fraudulent schemes (Carlson 2007). Adding to the risk factors, during COVID-19, most businesses and work shifted to remote online mediums, which increased exposure to online fraud of older adults. In addition, scams are getting increasingly sophisticated, and scammers intentionally target senior citizens as potential victims of online fraud (Lazarus et al. 2024; Robinson and Edwards 2024). Overall, while older adults are less likely to be victims of violent and property crimes, they face a relatively higher risk of falling prey to financial scams compared to younger individuals. This underscores the need for targeted efforts to protect older adults from financial exploitation and to raise awareness about common scam tactics.

Grounded in the Bioecological Systems Framework (BESF; Bronfenbrenner 1979), this research explores the factors contributing to victimization, including

the ease of exploitation, the situational factors that set victims up for scams, their vulnerabilities, the dynamics within their environments, and the challenges victims face in recognizing scams.

The BESF was developed to explain human developmental issues such as the person–environment interaction in social work (Siporin 1980), runaway sexual minority youth pathways (Crawford 2018), and intercultural education research (Tong and An 2023). Only a few research studies have used the framework for aging-related societal issues, notably *aging-in-place* initiatives (Greenfield 2012).

Former studies examined elder financial exploitation committed by individuals close to the victims such as relatives and family members. Although these studies used the BESF model to conceptualize elder victimization, contrary to our study, they only studied cases where there was an expectation of trust in the relationship between the victim and the offender. For example, Vincenti and Maurya (2023) used the BESF model to conceptualize relatives' understanding of perpetrators of elder family members' financial exploitation, and Nguyen (2021) utilized the BESF to examine older people's information technology use and how that can be a risk or protective factor against financial exploitation. Others also utilized the BESF, to study the barriers of older people's utilization of home- and community-based services (Garza 2018). To our knowledge, no research has applied the BESF to explain victimization of older people by strangers. Moreover, previous research on older victims only focused on microsystemic characteristics such as personal characteristics (Coluccia et al. 2020; Bayne et al. 2023; James et al. 2014; Parti 2022; Shang et al. 2022), trustful relationships (Blomberg et al. 2016), and exosystemic issues such as awareness-raising campaigns and programs (US Department of Justice 2023).

Hence, our paper is the first known attempt to discuss the lesser explored meso-, macro-, and chronosystemic findings within the BESF in the context of older people's scam victimization. In doing so, we comprehensively categorize older victims' vulnerabilities and needs to help refine prevention and intervention policy.

Our exploratory research involved interviewing victims directly ($n = 19$). Communicating directly with online scam victims is vital for several reasons: it helps to identify both the reasons for underreporting and the needs of victims, particularly in older individuals (Parti and Tahir 2023); it elucidates the challenges of reporting, the lack of support services available, the devastating impact online fraud has on victims, and the need for more effective responses and support mechanisms (Cross et al. 2016); it challenges the victim-blaming (Cross 2014) and agist discourse (Lazarus et al. 2024); it provides insight into the reasons as to why victims fall for online scams in the first place, such as the display of authority or legitimacy by scammers (Button et al. 2014); it helps to explore the psychological impact of online dating romance scams, including losing a relationship (Whitty and Buchanan 2016; Robinson and Edwards 2024; Lazarus et al. 2023); and it advocates for a more effective and victim-centered response to cyber fraud and scams (Button and Cross 2017; Bilz et al. 2023). To date, few studies have tried to untangle the intricate realities of scam victims by speaking directly with victims (Blomberg et al. 2016; Cross et al. 2018; Cross 2018a). This is especially true for older victim groups (Cross 2015), due to their relative inaccessibility and reluctance to report (DeLiema et al. 2020),

and their reticence toward sharing experiences (Parti and Tahir 2023). The current paper adds to the literature by filling these gaps.

Theoretical framework

Ecological frameworks emphasize the dynamic transactions between individuals and the environmental contexts that shape continuity and change across their lifespan (Satariano 2006). Urie Bronfenbrenner's (1979) bioecological systems framework (BESF) emphasizes the importance of various environmental systems and how they influence individual behavior and development. BESF divides the environment into five interconnected and co-existing systems, namely microsystem, mesosystem, exosystem, macrosystem, and chronosystem (Bronfenbrenner 1979: 3).

The innermost circle is the *microsystem*, referring to the immediate environment in which an individual lives and interacts. For an older person, this could include their family, close friends, and daily social interactions. The quality of these relationships can significantly impact a person's vulnerability to scams. For example, strong, trusting family relationships may protect against scams by providing timely advice and intervention (James et al. 2014). In addition, familial trust fosters an environment where seniors feel comfortable seeking guidance on financial matters, reducing the likelihood of them making hasty or uninformed decisions. In addition, family members can actively monitor elderly relatives' financial activities, identifying and addressing potential scams before they cause significant harm (Kokorelias et al. 2019). In contrast, social isolation can increase vulnerability (Kang and Ridgeway 1996; Button et al. 2024b). Alves and Wilson (2008) indicated that individuals between the ages of 60 and 70 register notably higher scores on the Revised UCLA Loneliness Scale and the Emotional Social Loneliness Inventory compared to other age groups. Correspondingly, telemarketing scams disproportionately affect these adults (Kang and Ridgeway 1996). The isolation they experience often propels individuals to seek out social connections, increasing their propensity to engage with unfamiliar people. This can lead to a greater likelihood of being deceived by fraudulent schemes (Alves and Wilson 2008; Robins and Edwards 2024).

Microsystemic circumstances also include the personal characteristics of the studied population. Personality traits like being kind (Robinson and Edwards 2024), impulsivity and low self-control can increase one's susceptibility to being scammed (Borwell et al. 2018; Kirwan et al. 2018; van Wilsem 2013). Being more active online and using certain payment methods, such as money wire transfers, can also be a risk factor (Emami et al. 2019). Demographic characteristics such as education and race can also make certain groups more vulnerable (Garg and Nilizadeh 2013).

Individual differences and psychological factors such as gender, age, familiarity with the sender, and awareness of phishing risk potentially impact the success of detecting scams (Williams et al. 2017). Norris et al. (2019) also suggest that personality traits, time-limited messages, and mood states have a potential impact on fraud susceptibility. Therefore, it is essential to identify those individuals most at risk and provide targeted consumer education measures to prevent victimization (Norris et al. 2019; see also Whitty 2019).

The second layer is the *mesosystem*, involving the interconnections between the microsystems in a person's life. For older adults, this could include the interactions between their family dynamics and community services. How these entities collaborate or fail to do so can influence a person's risk of being scammed. In a qualitative study of older people's scam victimization in Virginia, Parti and Tahir (2023) found that the prosocial, supportive nature between a victim and their community accelerated emotional reconciliation among victims, even when the financial loss was not recovered.

Cross et al. (2016), Cross (2015), and Arumugam et al. (2021) also underscore the importance of proactive and cooperative policing and support for victims. Cross's (2018b) study in Australia identified a variety of misconceptions and unrealistic expectations around the capabilities and practices of the fraud justice network regarding online fraud. Unmet expectations of law enforcement agencies' ability to respond appropriately or adequately can significantly contribute to a victim's trauma and cause unwarranted anger and frustration toward law enforcement agencies (Cross 2018b). In a subsequent study, Cross (2020) found that pertinent organizations fail to exchange information or work together synergistically to eliminate scams, which can indirectly affect a victim's propensity to report.

The next layer is the *exosystem,* which encompasses the larger social system affecting—yet not directly containing—the individual. This could include policies on elder care, law enforcement effectiveness, and community awareness programs about scams. Government reports (NCA 2020) assert that victims of cybercrime were unlikely to report crimes immediately due to the perception that police were ill-equipped to deal with such offenses. In addition, these reports identify policing issues including a lack of cybercrime knowledge. Because of the anonymous nature of the internet, investigators cannot obtain accounts from victims or witnesses, meet their needs, identify potential sources of evidence (e.g., personal computers), or otherwise progress the investigation (Curtis and Oxburgh 2023). A lack of professional resources by law enforcement leads authorities to pass cases between organizations or departments with little apparent interest (Button et al. 2020).

In the past 2 decades, various interventions have been proposed to combat online scams, with varying degrees of effectiveness, although evaluation is scarce (Button et al. 2024a). Research highlights the potential of training interventions and blacklisting techniques in detecting phishing websites. For instance, Alnajim and Munro (2009) proposed and evaluated a novel anti-phishing approach that uses training intervention for phishing website detection. Ludl et al. (2007) recommend a classification model to explore web page properties in order to help identify phishing pages and differentiate between malicious and legitimate pages. However, Button et al. (2024a), reviewing different tools and strategies, emphasize that the prevention model should be complex, incorporating individual, community and organizational levels, and involving cooperative partnerships between communities, law enforcement, financial institutions and tech companies.

The *macrosystem* is the cultural or societal blueprint that encompasses the individual. It includes societal beliefs, values, customs, and laws. Cultural norms and attitudes around respecting or neglecting older people play a significant role. Beyond financial loss, online fraud can impact mental and psychological well-being (Bilz et al. 2023; Cross 2019). This is especially concerning for older individuals,

who can disproportionately suffer from self-blame as a consequence of online fraud targeting or victimization (Button et al. 2024b). Furthermore, victims often experience various physical health issues resulting from the fraud (Cross 2019). Victims may also feel guilty or troubled by the disappointment of their children, who may have expected an inheritance that was lost to the fraud (Cross et al. 2016).

Button and Cross (2017) argue that there is a need for a victim-centered approach to tackling cybercrimes, and that this is achieved by listening to the voices of victims. They challenge the common discourse against online victims, which labels them as gullible, greedy, and lacking in technological and social savviness. This discourse unfairly places blame on the victim for failing to recognize the fraudulent nature of the situation (Button and Cross 2017), and dismisses the importance of their perspective.

The *chronosystem* is the outermost layer within the BESF. It includes the dimension of time, reflecting the personal and environmental changes that occur during a person's life. For older adults, this might involve changes in cognitive abilities, health status, or social roles that increase their vulnerability to scams. Prensky's (2001) concept of "digital immigrants" offers a framework for understanding how different generations engage with digital technology. Digital immigrants, according to Prensky (2001), are individuals who were not born into the digital world, but have adopted some aspects of new technology at some point in their lives. In contrast, "digital natives" have been immersed in digital technology from a young age.

Research points to the importance of digital literacy development in scam prevention (Graham and Triplett 2017), especially among older people (Moore and Hancock 2022; Shang et al. 2022). Digital literacy is not just about knowing how to use technology, but also about understanding how to navigate its content critically (Ng 2012). Digital immigrants may not always possess the critical literacy needed to discern legitimate communications from scams (van Deursen and van Dijk 2009, 2011; Helsper and Eynon 2013). They may be more likely to take information at face value without verifying its authenticity, making them more vulnerable to phishing, fraudulent websites, and other digital scams. This characteristic of digital immigrants, paired with their preference for more direct communication in general (e.g., talking on the phone instead of reading emails or text messages; Button et al. 2024b), makes them more vulnerable to online imposters. In addition, while younger people are typically more immersed in the cyberworld as an integral part of their lives, older age groups might only use it when necessary (Tinmaz et al. 2022). Hence, older generations may fail to utilize social media as an information source essential to enhancing digital literacy. In addition, they frequently hail from a generation where the values of interpersonal trust and community goodwill were not merely encouraged, but deeply woven into the social fabric (Bayer 2022; Clark and Lewis 2017). This cultural ethos, which emphasizes the importance of trustworthiness and the benefit of the doubt, is intentionally exploited by scammers (Lazarus et al. 2024) adept at employing advanced social engineering techniques.

In the following sections, we present the sample, the methods, and the results incorporated into the BESF. We also discuss the findings along with policy recommendations. Our goal is to help navigate the complexities of scams' impact on older adults and present the findings in a novel way that helps reform prevention and policy initiatives.

Sample, methods, and design

By drawing from the victims' narratives, the interpretive phenomenological approach (Smith et al. 2009; Smith 1996) allows for an inclusive representation of participants' and researchers' viewpoints of these events. Interpretive phenomenological analysis helped explain the underreporting of scams by factoring in the victims' perspectives, and the meaning they attach to the experience. It focuses on the lived experiences of the respondents, and how their scam victimization affected their lives.

The research targeted individuals aged 60 years and above, encompassing those directly victimized by scams. Initial participant recruitment involved a survey distributed online via the Virginia Chapter of the American Association of Retired Persons (AARP) and at senior living facilities in Virginia. Subsequent efforts included a snowball sampling element; outreach at local farmers' markets and facilities, and participant referrals by interviewees. The justification for using different sample strategies is, as Patton (1990) emphasizes, to maximize the number of participants and gather information-rich data for a systematic study (cited in Bailey 2007, pp. 64–65). As a result of the multiple-step sampling strategy, we conducted 19 in-depth interviews: 16 with victims in the summer of 2021, and an additional three in the summer of 2023 with individuals newly referred to us by previous participants. The 16 interviews conducted in the summer of 2021 were part of a larger research project of the authors (Parti and Tahir 2023). As the literature suggest, re-analyzing data, with new research questions, is a legitimate way of data utilization and it can also provide new insights and enhance depth of understanding (Van Den Berg 2005; Saldana 2015). Out of the 35 interviews we originally conducted in the larger project (anonymized), this paper only re-analyzes those conducted with primary victims, leaving out interviews with victims' family members as secondary victims.

Interviews ranged from 21 to 64 min, with a 35-min mean length. Most interviewees ($n=11$) identified as female, with eight males. All participants were white/Caucasian, ages ranging from 62 to 91, with a 72.5 mean age. Most participants ($n=16$) held college degrees or higher (three participants' highest level of education remained unknown). None of them was diagnosed as having cognitive impairments at the date of the interview. All participants were victimized by scammers and suffered financial and/or emotional harm as a consequence. The research team applied a semi-structured interview protocol containing demographic and victimization-related questions: (1) were you victimized by scammers in the past 12 months? (We defined scams to participants as "online or telephone fraud where you receive an unsolicited call, text message, social media message or email from an unknown individual asking you to send money, verify or share sensitive information offering non-existing or fraudulent services or relationship in return") (2) When did you realize you have been scammed? (3) Did you suffer from any harm (financial or emotional)? (4) Did you ask for help or report it to anyone? (5) Did you receive any helpful response? (6) Do you think older individuals might be vulnerable to scams? (7) What do older scam victims need? (8) Have you seen any anti-scam presentations or prevention programs? What did you like in them? How would you suggest to further develop these presentations or programs? Lastly, we asked participants

Table 1 Research findings categorized into types of ecosystems

Type of ecosystem	Vulnerabilities	Findings of our study
Microsystem	Being alone (not having trusted family members or friends around) Social isolation	Victim characteristics: higher than average education level, high relative level of computer savviness, no individuals diagnosed with cognitive decline The high-level sophistication of scams they experienced made it relatively easy to exploit participants Strong relationships with family members were crucial in identifying the red flags, and in resolving the situation quickly
Mesosystem	Anticipation of in-person or personalized contact and interaction	Intervening/confounding dynamics in the older person's environment either enabled or disabled resolving the conflict and getting closure, e.g., personalized contacts with reporting agencies, feedback, and reassurance
Exosystem	Not knowing where to report, and not having impartial consultants around	Awareness-raising programs are complicated, poorly accessible, and often use jargon
Macrosystem	Subject to intersectional victim blaming and agist stereotyping	Being open about victimization was hindered by the anticipation of victim blaming and stigma Self-blame also hindered being public about victimization
Chronosystem	Trusting too much; perceiving phone and internet as trustworthy sources for legitimate information and communications	Trust as a generational issue Digital immigrants (Internet as a relatively new medium that older generations did not grow up with)

to rate their computer savviness/literacy on an imaginative scale and demographic information such as age, gender, and highest education. All participants actively consented to the interview.

The Virginia Tech Institutional Review Board approved the study under #21-415. Due to the COVID-19 pandemic, and accessibility issues, interviews were conducted through video conferencing platforms. Participants were provided with an informed consent form, ensuring voluntary participation and confidentiality, with no compensation offered.

Interviews were recorded and transcribed through Zoom and Otter.ai software and human assistance, and then subjected to line-by-line coding using Atlas.ti v. 9 software. We applied thematic analysis using the stepwise method of Braun and Clarke (2006), including repeated readings, the generation of initial codes, and the identification of main themes. Multiple team members independently coded interviews, and the research team further discussed codes and themes for intercoder reliability. This comprehensive methodological approach enabled a nuanced understanding of participants' experiences. In the coming section, we present our research results by categorizing the answers into the five large systems of the BESF (Table 1): (1) What factors contributed to victimization?; (2) What were the confounding or intervening

factors of their environment that enabled or hindered the conflict's resolution?; (3) What help or response did they receive, and from whom? And was such help/response useful?

Results

Microsystem 1—the personal characteristics and vulnerabilities of victims

How easy was it to exploit the victims?

Participants had both relatively high levels of education and computer savviness (participants estimated their computer savviness between 3 and 5 on a 1–5 Likert scale, where 3 meant "average" and 5 meant "advanced" with computer programming and website management skills; $M = 3.73$). In addition, all participants kept their fraud knowledge updated by participating in specific trainings provided by local universities, the Agency on Aging, AARP, or even by their employers. Despite the high level of education and computer literacy, it was relatively easy to exploit victims because of the sophisticated nature of the scams they encountered (Lazarus et al. 2024). For example, a participant (Interviewee #1) who even taught computer security classes and judged her computer knowledge at level 5, received a phishing email with a link to a website offering an excellent financial deal. Both the email and the website looked legitimate. Still, somewhere down the line of transactions, the website asked for too much private information (e.g., social security number) that was not necessarily needed for the transaction. This participant suffered financial and emotional harm by only recognizing the red flags late.

Another participant received a call from scammers who pretended to be the participant's bank. They told him there was an accidental overpayment of interest, and the victim could "straighten it out" by transferring the overpayment to the bank. The scammers kept putting the victim on hold, as the victim's bank was on their other line, and they intended to get the identifying information piece by piece from the victim waiting in the other line. Finally, the actual bank called the victim to check the legitimacy of the proposed transactions. The participant, who estimated his computer savviness at 3.5, also became suspicious of the process, and he did not lose money; nevertheless, it was a sophisticated scam attempt.

Another participant received a phishing email from scammers pretending to be his pastor. The scammers knew the victim's church, the pastor's name, knew about their trusted relationship, and even spoofed the pastor's email address. They asked the victim to buy gift cards, scratch the numbers, and send photos of them. The participant, who estimated his computer literacy at 3.5, did not follow the scammers' requests because he had heard about this particular type of scam. However, the scammers knew intricate details that enabled them to boldly attempt to exploit a trustful relationship.

Another participant, a retired university professor with a self-estimated level 3 computer literacy score, received a phone call from imposters pretending to be the victim's daughter. The daughter was crying; she said she had been in a car accident,

and she needed the victim to pay for the ER service of the injured party, as well as for her bail, as she was going to be arrested for causing the accident. The victim also talked to an alleged police officer at the scene and, in a later call, with an alleged local bail officer to whom the victim was supposed to pay the bail money. The scammers knew where the victim and her daughter lived (the calls came from matching area codes), knew the daughter's name, and imitated her voice so successfully that even her mother (the victim) believed it was her. It was a concerted effort of multiple scammers who even used traffic and ER background noise to make the call more authentic. If the victim had not called her daughter's husband to talk to him before taking out the money, she would have lost thousands of dollars.

Vulnerabilities

When asked about the vulnerabilities that possibly added to the risk of their victimization, we grouped participants' answers into two distinct categories: (1) being alone, and (2) trusting too much. Being alone meant that the individual was physically alone or not in proximity to close family members who could have signaled the red flags at the time of the scam. In asking them about these vulnerabilities, our participants' answers included:

> Not paying attention that day." (Interviewee #11)
> Not having anyone around who would ask, 'What are you doing?'" (Interviewee # 15)

As it was posited by previous studies (Lichtenberg et al. 2013; Robinson and Edwards 2024), loneliness and looking for friends were other factors of vulnerability. In a romance scam, a participant started a distant relationship with a scammer who approached her on social media. This participant was still active; she was a member of several committees in her living community and had an active business. She was well educated and had an exciting and colorful life. She wanted to believe that continuing such a lifestyle was possible despite her knowledge about scammers potentially preying on people via social media (Bilz et al. 2023):

> "*I was isolated, I was lonely. But after the life I lived, I needed adventure and impulsivity. You know, if you lived a life full […], where those things [relationships] are normal, you'll need to continue that…*" *(Interviewee #14)*

Losing loved ones, especially spouses, also tended to put participants on the verge of desperately seeking a person who could fill that sense of loss, corroborating previous findings (Robinson and Edwards 2024). As participants put it:

> "*I was kind of lonely. And so, to get daily 'Oh how are you?', you know, just daily contacts! It was good for me because I was thinking, 'Oh, someone cares.'*" *(Interviewee #18)*
> "*I'm on Facebook, with almost 1,000 friends. I do very little posting. But I do wish each of these friends a happy birthday. I have to be involved at least for doing that.*" *(Interviewee #15)*

Chronosystem—trusting too much as a generational characteristic

Trusting too much, the other significant vulnerability participants mentioned, entails both people and technology (Coombs 2014; Titus and Gover 2001). Although they all used email as a means of communication, they shared that being part of a generation that pursues more personal communications over non-personal or online communication leads them to be more likely to answer cold calls than not. As another generational issue, the telephone was frequently mentioned as something that one can trust (Button et al. 2024b):

> "*I think there's probably something in older people's minds… the phone. The landline, that is. I've had it for more than 60 years. And it's always been reliable… you naturally pointed toward trusting anything that comes in over the phone.*" *(Interviewee #11)*
> "*If you are used to dialing up your sister or friend in Wyoming or whatever, you know, it's there, you can just reach for it and do it. But these scammers have turned your friend into an enemy.*" *(Interviewee #11)*
> "*They didn't start using computers, oftentimes until they were in the middle of their careers, and [even then] they were forced to use computers because of our jobs… […] I know I must call those people if I really want to get some information from them.*" *(Interviewee #14)*

Interviewees also mentioned age as a factor that hinders one's adaptability and preparedness. For our participants, being "old" meant less adaptability to ever-evolving scams, and made them less likely to "be on the lookout" for scams at all times. Although all participants were still active in their communities and sometimes in their jobs, juggling these daily activities and duties could lead them to become less attentive in "untrustful" situations. In addition, according to our participants, there is a difference between age groups and generations in how they process information. They referred to their generation as one that did not have the internet when they were younger and more adaptive. They noted that they will always have the "handicap" of anticipating trustful relationships and information online because they socialized for most of their lives in the offline world, where the chance of encountering a fraudster was significantly lower than it is online. Thus, they are more likely to view emails and online news as legitimate services, as compared to younger generations:

> "*That's a function of… not age necessarily, but of the time at which email on the computer became a part of our daily lives when I was much younger… That's all something we've all learned to use. Some people were born into it, other people had it all of a sudden…were like, 'Oh, what's this?'*" *(Interviewee #4)*
> "*I think a lot of older people are just afraid, you know, we didn't grow up with this. This is all pretty new, and we are just afraid of it.*" *(Interviewee #12)*
> "*These are folks that professionally never used computers until the very end and all they did was word processing, that kind of thing… they just don't understand the dynamics.*" *(Interviewee #8)*

Others mentioned that "offline" socialization affects people's level of trust in others and impacts how they process information. Participants asserted that there is a generational gap concerning the level of trust in people and the credibility of conversation partners:

> "*The generation older than me is very trusting… they lived in a world where you assume the best of people. And only lost that trust if they made you lose that trust.*" *(Interviewee #8)*

Microsystem 2—relationships with family members

At the same time, trust in others can positively impact resilience. In particular, if participants maintained trustful relationships with their families, it enabled them to resolve the situation quickly and without a significant amount of financial loss. Trust was demonstrated by the relative ease with which they reached out to family members despite strongly negative feelings surrounding their victimization, such as shame, embarrassment, confusion, and loss of self-esteem (Whitty and Buchanan 2016; Button et al. 2024b):

> "*Something like that involves the whole family because usually it's the kids that have to sort of bring their parents along.*" *(Interviewee #8)*

Participants also emphasized the need for trustworthy individuals in situations where significant financial and emotional harm is at risk. Some participants identified trusted friends as a "safety network" that regularly checks in on them. Others emphasized that trusted individuals helped them to identify red flags and process victimization in a healthier way:

> "*Every day, when you work, and you are supposed to show up at work […] usually someone at work is going to try to call and find out what's going on with you. So, you have those checks. But when you're retired, and […] if you don't have friends to check on you, friends you're supposed to meet, […] there is just no backup, no safety net there.*" *(Interviewee #14)*
> "*So, I said [to my husband] Hang up! [But] I didn't really have anyone close that I could just run by.*" *(Interviewee #19)*
> "*I actually had my daughter and son-in-law living with me, but they just happened to be away that day. And so no one was here to even say, 'What's going on?' or, 'Do you know what you're doing?' or, 'What's that call about?' or anything.*" *(Interviewee #15)*
> "*I think [family provides] reassurance that these are pretty simple [to solve], depending on the type [of scam]. The bottom line is everyone needs a strong family, you need people that are close to you to help out.*" *(Interviewee #10)*
> "*I think the support of family and friends, and having family and friends be aware when you're getting older and maybe less able to be frank with people to say, 'Look, I don't know you, I can't share this information.'*" *(Interviewee #5)*

Sometimes the age-related vulnerabilities of digital immigrants are connected to the need for trusting relationships. Friends and loved ones can help mitigate the burden that comes with the emotional harm of victimization:

"*In our age group,… [in] a lot of cases, emotional support from family would be key. And to help us regain what we had [lost]. (Interviewee #1)*

Mesosystem—dynamics behind resolving the conflict

The mesosystem encompasses those intervening or confounding dynamics in a victim's environment, which enable or disable resolving the conflict and getting closure. Participants pointed to two distinct directions regarding intervening dynamics in the targeted person's environment. When participants managed to establish contact and talk to a human being instead of filing a non-personalized report or form, they appreciated it and took it as constructive and helpful. Furthermore, if there were trusting family members who listened and constructively helped resolve problems (e.g., screened the computer for scam backdoors and viruses, and facilitated the reporting to the authorities), that was also interpreted as a helpful response. Constructive help meant helping to report the incident, making sure that the incident would not happen again, regularly checking in on the older relative, and doing all this without making the victim feel blamed. Personified communication and feedback were helpful even if the money was gone:

"*I wrote out a long kind of explanation of how it happened. And we got it over to the… police department. I talked to them on the phone.*" *(Interviewee #8)*
"*They [the police] were not equipped to chase that stuff so… I think they moved up to the state level. But I got to talk to them, and it helped me find closure.*" *(Interviewee #8)*
"*She called the cops and we were able to get some helpful information.*" *(Interviewee #14)*

It also helped achieve closure when the victim's family members and the authorities (e.g., law enforcement, adult protective services, and long-term care ombudsman) cooperated, and, as a result, the victim received personal attention and feedback:

"*They had the police department visit and sit down with me, and it was good to hear their take on the case.*" *(Interviewee #3)*
"*I got in touch with the sheriff. We live in a tiny county… and the sheriff is kind of a buddy. […] I called him right away and he said, 'Are you in any danger right now?' And I said, 'No.' And he said, 'Absolutely don't give any money to anyone.' That was the most he could do for me. But it was good to know that he was there, listening.*" *(Interviewee #19)*

In contrast, when the agency or person to whom the incident was reported did not provide feedback, was impersonal, or communicated poorly, participants deemed the help counterproductive:

"*I've reported a couple times to the FBI, but you never get any feedback. And you know, maybe it comes across somebody's desk and they go, 'Yeah, that's another one.'*" *(Interviewee #10)*

An important takeaway is that victims anticipate more personal connections:

"*There need to be people who are there to listen to your experiences and […] maybe they're the ones who help you determine whether to take it further.*" *(Interviewee #2)*
"*I think more face-to-face contact. […] I think seniors still like that connection with a real person. You know, they can read the computer screen, but if you tell them that—and even by Zoom —I think it would be helpful.*" *(Interviewee #11)*
"*The older folks get, the fewer they have any kind of ability to really understand it and [they] get less comfortable with the idea of, you know, reporting things electronically. [Rather than] figuring out which buttons to push, they're more comfortable on the phone. I think a phone line that gets answered by a human that can take a report.*" *(Interviewee #7)*

Exosystem and macrosystem—larger social dynamics

The exo- and macrosystems encompass the more extensive social system affecting an individual, even if they are not directly working with them. This could include community awareness programs about scams, and societal attitudes toward older people in general. Participants acknowledged that a wide variety of awareness-raising programs and information sessions are available locally, regionally, and on the state level. However, they criticized programs for not speaking directly to the victim's needs, and for their oftentimes convoluted language and poor accessibility:

"*It's buried in language that is hard to understand and it's full of buzzwords, and you know if you're reading something, even if it's just a paragraph, and you hit that second word you don't understand, you're done.*" *(Interviewee #8)*

The same participant recommended that awareness-raising webinars would need to involve interacting directly with the audiences:

"*If they really want to attack this problem, they're going to have to do better at communicating what the problems are to the people that are on the other end of the screen.*" *(Interviewee #8)*

Societal attitudes toward older scam victims can encompass victim blaming and stigmatization. These attitudes can amplify shame and self-blame, and oftentimes hinder victims from reporting or even talking to someone about their experiences. Participants talked about these circumstances in the interviews:

"*In this small community, I want to give voice, definitely, to help others, but at the same time, it's just something that's a little embarrassing. And I mean, you can get labeled… as someone who may cry wolf.*" *(Interviewee #15)*

"*Would be nice if people were all understanding. I'm too embarrassed that I fell for this. You know, I'm sorry, I really shouldn't… I should be a lot smarter than what I am.*" *(Interviewee #16)*
"*A one-on-one Zoom meeting like this would be helpful… It would lower the embarrassment factor, and you still would be able to talk about what an imbecile you had been [laughs].*" *(Interviewee #8)*

Discussion

In a departure from medicalized discussions of elder financial abuse (Patel et al. 2021; Worrilow and Barraco 2015; Price et al. 2011), we steered our interviews toward a novel approach rooted in the ecosystems surrounding the older person. To our knowledge, our study is the first attempt to analyze older people's vulnerabilities to scams committed by a person unknown to the victim, within the broader context provided by Bronfenbrenner's Bioecological Systems Framework (1979). Attaching the findings into the different systems within the framework, this paper recognizes the complexities of elder vulnerabilities and helps designate potential support systems. We also utilize the findings to form policy recommendations.

Our analysis of the circumstances of scam victims revealed that individuals acted within the bounds of reason. In addition, our sample was of highly educated retired people who exhibited educational attainment surpassing both Virginia and U.S. averages. Notably, participants self-reported no cognitive deficits, and they estimated their computer literacy to be relatively high. Still, modern cybercriminals' intricate and highly sophisticated techniques (Lazarus et al. 2023) have rendered such individuals susceptible to exploitation. In addition, our findings show that current methods of assisting older people in recovering from scam victimization are inadequate and demand thorough reevaluation.

Two primary vulnerabilities emerged from participant responses at the *microsystemic* level: "aloneness" and overtrust. Aloneness, in this context, refers to the absence of close family members or a general sense of solitude and isolation at the time of the scam. Victims often disparaged themselves for being deceived, expressing that if relatives had been present to alert them about red flags, their victimization might have been averted.

The vulnerability deriving from loneliness, especially among those seeking companionship, was a notable risk factor, corroborating previous findings (Kang and Ridgeway 1996; Alves and Wilson 2008). This finding is reflected in recent romance scam research (Robinson and Edwards 2024) positing that negative life events such as losing a loved one and widowhood increase susceptibility. However, nurturing family ties mitigated the risk of isolation, which proved vital in promptly addressing and resolving the scams with minimal financial repercussions, as seen in previous studies (James et al. 2014; Kokorelias et al. 2019). The strength of these relationships was evident in the ease with which victims could confide in relatives, overcoming shame and a compromised sense of self-worth.

In addition, the vulnerabilities associated with being less digitally adept—often seen in older age groups—highlight the importance of having trustworthy connections.

In examining the *chronosystem*, participants identified excessive trust as a pronounced vulnerability (Bayer 2022; Clark and Lewis 2017; Carlson 2007), affecting their interactions with both individuals and technology. Despite regularly using email, they expressed a generational preference for more personal encounters over impersonal digital communications, which, on the other hand, increased their susceptibility to responding cold calls. Often our participants regarded the telephone as a trustworthy device, contrary to their perception of newer technologies. The phone, especially the landline, proved to be a vital means of connection to family and friends. If that is compromised, they lose the only link to a social life, as Button et al. (2024b: 14) point out.

Participants recognized a generational gap in information processing, describing themselves as growing up without the internet. Their lack of early digital socialization resulted in their approaching online relationships and information with an inherent trust, reminiscent of an offline world where the likelihood of encountering a scammer was reduced. As a result, older adults may be more inclined to treat email messages and online news as inherently legitimate, a perspective differing from their younger, more digitally skeptical counterparts.

Unlike younger generations who engage with social media as an integral part of their daily life, older adults tend to utilize digital platforms out of necessity. Their interactions with the digital world are often the result of attending to practical matters such as scheduling appointments, conducting business, or managing administrative tasks. This limited engagement results in reduced exposure to the frequent updates and cues that could signal the presence of scams, leaving them at a disadvantage.

The landscape of scams is one of relentless change and complexity, presenting a particular challenge for those termed "digital immigrants" (Prensky 2001). These individuals often find it arduous to stay abreast of the continuously evolving deceitful tactics scammers employ. It is of no surprise that internet users with only a few years of online experience are particularly exposed to scams due to limited fraud awareness (Saad et al. 2018). Moreover, the rapid pace of technological change means that social media platforms are not always designed with older users in mind, leading to their exclusion from these essential sources of information and community. As social media becomes a primary channel for staying informed and connected, the digital divide may widen, with older populations becoming increasingly vulnerable to misinformation and cyber manipulation. To mitigate this risk, a clear and immediate need exists for inclusive technology and targeted educational initiatives to help older individuals become more adept and vigilant in their digital interactions (Button et al. 2024a). Nevertheless, younger generations ("digital natives"; Prensky 2001), are too, must be aware of scams targeting older adults, for several reasons. First, as they age, they too become potential targets for these scams and need to stay updated on evolving scam tactics and manipulation strategies used by scammers (Button et al. 2024b). Second, they are integral members of families, often acting as caregivers or support systems for their older relatives. As

our research suggests, younger family members can play a crucial role in preventing and intervening in scam attempts against older adults. Their involvement can help safeguard the financial and emotional well-being of older family members, fostering a safer and less victim-blaming family environment. Recognizing these threats ensures a holistic approach to family security.

Within the *mesosystem*, the dynamics that either facilitated or hindered the resolution of fraud and the attainment of closure for older individuals were scrutinized. The interviews revealed two main pathways in the environment of the targeted individuals that influenced the outcome. Positive outcomes were associated with personal interactions; participants found it constructive and helpful when they could speak directly to someone instead of submitting an impersonal report or form.

The presence of trusting family members who actively engaged in resolving the issue was also perceived as beneficial (Parti and Tahir 2023). Whitty and Buchanan (2016) found that victims often feel they cannot confide in trusted family members, friends, or colleagues out of fear of rejection and anger. Reflecting these previous findings, our participants found personalized attention and tailored feedback crucial, especially when both family members and authorities collaborated. Conversely, when the response from agencies or individuals to whom the scam was reported was perceived as judgmental, impersonal, unresponsive, or poorly communicated, participants felt the support was unconstructive and even damaging.

The *exosystem* or the broader social context includes educational campaigns on scams and the prevailing societal perceptions of older adults. Participants recognized numerous programs that raised awareness about scams at local, regional, and state levels. Nonetheless, they expressed concerns about these initiatives, noting that they often fail to adequately address the specific and unique needs of older victims. In addition, they pointed out that the language used in these programs can be overly complex and that there is a lack of easy access to the information provided. This finding corroborates Lazarus et al.'s (2024) concept of agism in prevention efforts according to which when it comes to developing cybercrime prevention tools, society chooses not to prioritize older age groups, as that would require more complex, coordinated, and costly solutions.

At the level of the *macrosystem*, agist attitudes and stereotypes about older adults play a pivotal role. This demographic often faces victim blaming and stigmatization, compounded by contradictory societal perceptions that equate age with both wisdom—implying that older individuals should "know better"—as well as with digital gullibility. Such perceptions erect a formidable barrier, preventing victims from reporting scams or seeking assistance due to fear of judgment, damage to their self-image, and loss of their autonomy.

Media representations often exacerbate the issue by portraying older individuals who engage in learning or embracing technology as anomalies (Ghosh 2023). Instead of reinforcing such stereotypes, there should be a concerted effort to create spaces and opportunities for older adults to learn and adapt. By fostering an inclusive environment where lifelong learning is normalized and supported, older adults can be better equipped to protect themselves against scams and feel empowered to speak out without fear of judgment or shame. By shifting how society views and supports the educational growth of older adults, it is possible to dismantle the stigma associated

with victimization and encourage a more open and supportive dialogue about the experiences of older scam victims. This societal shift is essential for empowering older adults to report scams without fear of ridicule or blame, and to recognize them not as outliers but as integral and evolving members of the digital community.

Limitations

Although this study gives voice to older scam victims and places the findings about victimization, susceptibility, and adequate responses into a multisystemic ecological framework, it has limitations. It only represents voices of victims residing in Virginia, and does not focus on demographics of race, gender, or socioeconomic characteristics beyond being above 60, and of having been victimized by scams. We applied multiple sampling techniques to reach out to a diverse pool of victims; however, we acknowledge that people with socioeconomic disadvantages (e.g., without internet access at the time of the interviews) did not have a chance to participate. It is imperative that future research tackle these issues by recruiting participants whose voices are less heard. Finally, the study has been conducted to gain a broad understanding of an understudied area of older people's scam victimization, hence, it was an exploratory study, identifying patterns of older people's scam victimization, and suggesting viewing the phenomenon within a broader framework, instead of handling it independently of the underlying circumstances. Thus, the study helped develop descriptive insights to subsequent studies but needs follow-up investigation. As exploratory research, this study involved a relatively small sample size, which holds potential for response bias. Future studies must follow up these initial findings with results more generalizable to the population in question.

Policy recommendations

Revisiting the methods employed to aid older victims of scams is imperative, as current strategies are insufficient. In contemplating alternative forms of support, it is crucial to disseminate the message that anyone can fall prey to these highly manipulative cybercrimes. The effectiveness of simple software or being a "digital native" as defense is overstated; scams are sophisticated, and technical proficiency alone does not guarantee immunity. Notably, vulnerability to online fraud is not a question of lacking digital skills—many younger victims are ensnared as well, and even technologically adept older individuals are not exempt from such deceptions (Button et al. 2024a). Bearing these in mind, a multi-faceted response is necessary, one that includes active listening to the victim (Parti and Tahir 2023) and the fostering of a community willing and able to dispel myths surrounding victimization, such as the erroneous belief that only the "mentally declining" or "old" are susceptible. This approach aligns with the bioecological systems framework, which suggests creating community-focused interventions that engage not only older people, but also those capable of intervening or providing support in critical situations.

Utilizing BESF, programs should be tailored to address the diverse needs of varying population groups, encompass all age groups and actively involve participants

in dialogue. Awareness should be raised through multiple channels such as social media, software applications, virtual games, interactive theatre (Keisari et al. 2020; Moore et al. 2017), and interactive awareness raising (Whitty 2019). Adhering to the principle of "Nothing about them without them" (Doucet et al. 2022), participatory action research is critical and appropriate. Programs must involve those directly and indirectly affected to ascertain the needs of victims and their communities. Such initiatives should target not only private individuals, but also service providers and agencies, including non-profits, financial institutions, and law enforcement at local, state, and federal levels (see Button et al. 2024a for a complex prevention model). Furthermore, these entities must be aware of one another's efforts, and collaborate to enhance their collective impact on servicing the community.

With an increasing population of older adults, it is incumbent upon policymakers across multiple levels of government (i.e., local, state, and national) to employ strategies that are less about talking *to* older adults and more about talking *with* them. Our study reveals that there is ample reason to have older adults, the persons most targeted and affected, become an important part of the conversation about and the solution to scamming. A notable example of such a program is Success After Financial Exploitation (SAFE) by Lichtenberg and colleagues (2019), which helps older adults make sense of their finances, and provides one-on-one services to older adults who have been victims of fraud and identity theft. In addition to providing expert, individual guidance, the program targets hard-to-reach older adults, such as urban African Americans. Only by employing such strategies will the scourge of elder financial scams diminish.

Funding The research received funding from Virginia Tech (Institute of Creativity Arts and Technology, the Center for Gerontology, and the Center for Peace Studies and Violence Prevention, and the Commonwealth Cyber Initiative in Virginia.

Declarations

Conflict of interest On behalf of all the authors, the corresponding author states that there is no conflict of interest.

References

Alnajim, A., and M. Munro. 2009. An anti-phishing approach that uses training intervention for phishing websites detection sixth international conference on information technology: New generations. 2009. https://doi.org/10.1109/ITNG.2009.109.

Alves, Linda M., and Steve R. Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of Elder Abuse & Neglect* 20:63–85. https://doi.org/10.1300/J084v20n01_04.

Arumugam, N., F. Mohamad, A. Shanthi, and S. Dharinee. 2021. A study on online shopping scams. *International Journal of Social Science Research* 10:22. https://doi.org/10.5296/ijssr.v10i1.19290.

Bailey, Carol A. 2007. *A guide to qualitative field research*, 2nd ed. Thousand Oaks: Pine Forge Press.

Bayer, Y. 2022. Age and social trust: Evidence from the United States. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3596456.

Bayne, A. E. A., C. Lancaster. Mumford, and J. Sheridan-Johnson. 2023. Technology-facilitated abuse among Americans age 50 and older: A latent class analysis. *Journal of Elder Abuse & Neglect*. https://doi.org/10.1080/08946566.2023.2197270.

Bilz, A., L. A. Shepherd, and G. I. Johnson. 2023. Tainted love: A systematic literature review of online romance scam research. *Interacting with Computers* 35:773–788. https://doi.org/10.1093/iwc/iwad048.

Blomberg, T.G., J.M. Brancale, G.B. Pesta, J.W.A. Ranson, and B. Campion. 2016. Elder financial exploitation in a large retirement community. Florida State University College of Criminology and Criminal Justice Center for Criminology and Public Policy Research. https://news.fsu.edu/wp-content/uploads/2016/12/elder-fraud-report.pdf. Accessed 11 February 2024.

Borwell, J., J. Jansen, and W. Stol. 2018. Human factors leading to online fraud victimisation. *Advances in Digital Crime, Forensics, and Cyber Terrorism* 26–45. IGI Global. https://doi.org/10.4018/978-1-5225-4053-3.ch002.

Braun, V., and V. Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3:77–101. https://doi.org/10.1191/1478088706qp063oa.

Bronfenbrenner, U. 1979. *The ecology of human development: Experiments by nature and design*. Cambridge: Harvard University Press.

Button, M., and C. Cross. 2017. *Cyber frauds, scams and their victims*. New York: Routledge.

Button, M., V. Karagiannopoulos, J. Lee, J. B. Suh, and J. Jung. 2024a. Preventing fraud victimisation against older adults: Towards a holistic model for protection. *International Journal of Law, Crime and Justice* 77 : 100672. https://doi.org/10.1016/j.ijlcj.2024.100672.

Button, M., C. M. Nicholls, J. Kerr, and R. Owen. 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology* 47:391–408. https://doi.org/10.1177/0004865814521224.

Button, M., D. Shepherd, C. Hawkins, and J. Tapley. 2024. Fear and phoning: Telephones, fraud, and older adults in the UK. *International Review of Victimology*. https://doi.org/10.1177/02697580241254399.

Button, M., L. Sugiura, D. Blackbourn, R. Kapend, D. Shepherd, and V. Wang. 2020. Victims of computer misuse: Main findings. University of Portsmouth. https://pure.port.ac.uk/ws/portalfiles/portal/20818559/Victims_of_Computer_Misuse_Main_Findings.pdf. Accessed 10 February 2024.

Carlson, Eric L. 2007. Phishing for elderly victims: As the elderly migrate to the internet fraudulent schemes targeting them follow. *The Elder Law Journal* 14:423–452.

Clark, M., and S. Lewis. 2017. Trust in the digital age. *Journal of Social Psychology* 8:299–310.

Coluccia, A., A. Pozza, F. Ferretti, F. Carabellese, A. Masti, and G. Gualtieri. 2020. Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health* 16:24–35. https://doi.org/10.2174/1745017902016010024.

Coombs, J. 2014. Scamming the elderly: An increased susceptibility to financial exploitation within and outside of the family. *Albany Government Law Review* 7:243.

Crawford, M. 2018. Runaway sexual minority youth: Comparative analysis using Bronfenbrenner and Foucault. *Theory in Action* 11:51–71. https://doi.org/10.3798/tia.1937-0237.1810.

Cross, C. 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21:187–204. https://doi.org/10.1177/0269758015571471.

Cross, C. 2018a. Victims' motivations for reporting to the 'fraud justice network.' *Police Practice & Research* 19:550–564. https://doi.org/10.1080/15614263.2018.1507891.

Cross, C. 2018b. Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime & Justice* 55:1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001.

Cross, C. 2019. "You are not alone": The use of peer support groups for fraud victims. *Journal of Human Behavior and Social Environment* 29:672–691.

Cross, C. 2020. Responding to individual fraud: Perspectives of the fraud justice network. In *The human factor of cybercrime*, ed. E. R. Leukfeldt, and T. J. Holt, 359–88. New York: Routledge.

Cross, C., K. Richards, and R. G. Smith. 2016. The reporting experiences and support needs of victims of online fraud. *Trends & Issues in Crime & Criminal Justice* 518:1–14.

Cross, C., M. Dragiewicz, and K. Richards. 2018. Understanding romance fraud: Insights from domestic violence research. *British Journal of Criminology* 58:1303–1322. https://doi.org/10.1093/bjc/azy005.

Cross, C., R. G. Smith, and K. Richards. 2014. Challenges of responding to online fraud victimization in Australia. *Trends & Issues in Crime & Criminal Justice* 47:1–7.

Curtis, J., and G. Oxburgh. 2023. Understanding cybercrime in 'real world' policing and law enforcement. *Police Journal: Theory, Practice & Principles* 96:573–592. https://doi.org/10.1177/0032258X221107584.

DeLiema, Marguerite, Martha Deevy, Annamaria Lusardi, and Olivia S. Mitchell. 2020. Financial fraud among older Americans: Evidence and implications. *Journals of Gerontology Series B, Psychological Sciences & Social Sciences* 75:861–868. https://doi.org/10.1093/geronb/gby151.

Doucet, Melanie, Harrison Pratt, Martha Dzhenganin, and Jordan Read. 2022. Nothing about us without us: Using Participatory Action Research (PAR) and arts-based methods as empowerment and social justice tools in doing research with youth 'aging out' of care. *Child Abuse & Neglect* 130 : 105358. https://doi.org/10.1016/j.chiabu.2021.105358.

Emami, C., R. Smith, and P. Jorna. 2019. *Online fraud victimisation in Australia: Risks and protective factors*. Australian Institute of Criminology Research Report. https://www.aic.gov.au/sites/default/files/2020-05/rr16_online_fraud_victimisation_in_australia-v3.pdf. Accessed 12 February 2024.

Faviero, Michelle. 2022. Share of those 65 and older who are tech users has grown in the past decade. *Pew Research Center.* https://www.pewresearch.org/short-reads/2022/01/13/share-of-those-65-and-older-who-are-tech-users-has-grown-in-the-past-decade/. Accessed 14 june 2024.

Federal Trade Commission. 2024. *Age and fraud.* Federal Trade Commission. https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic. Accessed 14 June 2024.

Garg, V., and S. Nilizadeh. 2013. Craigslist scams and community composition: Investigating online fraud victimization. *IEEE Security and Privacy Workshops* 2013:123–126.

Garza, L. 2018. Understanding barriers affecting elders' low utilization of HCBS: A multiple case study of HCBS social workers. *Northcentral University ProQuest Dissertations & Theses*, 10846954.

Ghosh, M. 2023. Female instagram elderly influencers countering the ageing narratives. *Humanities & Social Sciences Communications* 10:804. https://doi.org/10.1057/s41599-023-02323-4.

Graham, R., and R. Triplett. 2017. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior* 38:1371–1382. https://doi.org/10.1080/01639625.2016.1254980.

Greenfield, Emily A. 2012. Using ecological frameworks to advance a field of research, practice, and policy on aging-in-place initiatives. *The Gerontologist* 52:1–12. https://doi.org/10.1093/geront/gnr108.

Helsper, E. J., and R. Eynon. 2013. Distinct skill pathways to digital engagement. *European Journal of Communication* 28:696–713. https://doi.org/10.1177/0267323113499113.

Ianzito, Christina. 2024. *Many Americans worry about becoming scam victims, new report finds.* AARP. https://www.aarp.org/money/scams-fraud/info-2024/identity-fraud-report.html

IC3. 2023. *Elder fraud report*. Federal Bureau of Investigation. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf. Accessed 12 February 2024

James, Bryan D., Patricia A. Boyle, and David A. Bennett. 2014. Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect* 26:107–122. https://doi.org/10.1080/08946566.2013.821809.

Kang, Y. S., and N. M. Ridgway. 1996. The importance of consumer market interactions as a form of social support for elderly consumers. *Journal of Public Policy & Marketing* 15:108–117. https://doi.org/10.1177/074391569601500110.

Keisari, Shoshi, Anat Gesser-Edelsburg, Dani Yaniv, and Yuval Palgi. 2020. Playback theatre in adult day centers: A creative group intervention for community-dwelling older adults. *PLoS ONE* 15 : e0239812. https://doi.org/10.1371/journal.pone.0239812.

Kirwan, Gráinne. H., Chris Fullwood, and Brendan Rooney. 2018. Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior & Social Networking* 21:123–128. https://doi.org/10.1089/cyber.2016.0714.

Kokorelias, Kristina M., Monique A. M. Gignac, G. Gary Naglie, and Jill I. Cameron. 2019. Towards a universal model of family centered care: A scoping review. *BMC Health Services Research* 19:564–575. https://doi.org/10.1186/s12913-019-4394-5.

Lazarus, S., P. Tickner and M.R. McGuire. 2024. Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal.* ISSN 0955-1662 (In Press)

Lazarus, S., J. M. Whittaker, M. R. McGuire, and L. Platt. 2023. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology* 2 : 100013. https://doi.org/10.1016/j.jeconc.2023.100013.

Lichtenberg, Peter A., Latoya Hall, Evan Gross, and Rebecca Campbell. 2019. Providing assistance for older adult financial exploitation victims: Implications for clinical gerontologists. *Clinical Gerontologist* 42:435–443. https://doi.org/10.1080/07317115.2019.1569190.

Lichtenberg, P. A., L. Stickney, and D. Paulson. 2013. Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist* 36:132–146.

Ludl, C., S. McAllister, E. Kirda, and C. Kruegel. 2007. On the effectiveness of techniques to detect phishing sites. In *Detection of intrusions and malware, and vulnerability assessment*, 20–39. Berlin: Springer. https://doi.org/10.1007/978-3-540-73614-1_2.

Moore, Raeanne C., Elizabeth Straus, Sheena I. Dev, Steven M. Parish, Seema Sueko, and Lisa T. Eyler. 2017. Development and pilot randomized control trial of a drama program to enhance well-being among older adults. *Arts in Psychotherapy* 52:1–9. https://doi.org/10.1016/j.aip.2016.09.007.

Morgan, Rachel E and Susannah N. Tapp. 2024. Examining financial fraud against older adults. *NIJ Journal.* https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults#note15

Moore, Ryan C., and Jeffrey T. Hancock. 2022. A digital media literacy intervention for older adults improves resilience to fake news. *Scientific Reports* 12:6008. https://doi.org/10.1038/s41598-022-08437-0.

National Crime Agency (NCA). 2020. National strategic assessment of serious and organised crime. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file. Accessed 12 February 2024

Ng, W. 2012. Can we teach digital natives digital literacy? *Computers & Education* 59:1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016.

Nguyen, K.T. 2021. College-educated older adults and information and communications technology. *University of Southern California ProQuest Dissertations & Theses*, 28773427.

Norris, G., A. Brookes, and D. Dowell. 2019. The psychology of internet fraud victimisation: A systematic review. *Journal of Police & Criminal Psychology* 34:231–245. https://doi.org/10.1007/s11896-019-09334-5.

Parti, K. 2022. "Elder scam" risk profiles: Individual and situational factors of younger and older age groups' fraud victimization. *International Journal of Cybersecurity Intelligence & Cybercrime* 5:20–40. https://doi.org/10.52306/LIQS5025.

Parti, K., and F. Tahir. 2023. 'If we don't listen to them, we make them lose more than money:' Exploring reasons for underreporting and the needs of older scam victims. *Social Sciences* 12:264. https://doi.org/10.3390/socsci12050264.

Patel, Karan, Sean Bunachita, Hannah Chiu, Prakul Suresh, and Urvish K. Patel. 2021. Elder abuse: A comprehensive overview and physician-associated challenges. *Cureus* 13 : e14375. https://doi.org/10.7759/cureus.14375.

Patton, Michael Quinn. 1990. *Qualitative evaluation and research methods*, 2nd ed. Newbury Park: SAGE.

Prensky, M. 2001. Digital natives, digital immigrants, Part 1. *On The Horizon* 9:3–6. https://doi.org/10.1108/10748120110424816.

Price, Thomas, Patricia S. King, Rebecca L. Dillard, and James J. Bulot. 2011. Elder financial exploitation: Implications for future policy and research in elder mistreatment. *Western Journal of Emergency Medicine* 12:354–356.

Robinson, J., and M. Edwards. 2024. Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments. *Security Journal*. https://doi.org/10.1057/s41284-023-00410-4.

Saad, M. E., S. Norul, and M. Zamri. 2018. Cyber romance scam victimization analysis using routine activity theory versus Apriori algorithm. *International Journal of Advanced Computer Science and Applications* 9:479–485.

Saldana, J. 2015. *The coding manual for qualitative researchers*. Sage.
Satariano, W. A. 2006. *Epidemiology of aging: An ecological approach*. Sudbury, MA: Jones and Bartlett Publishers.
Shang, Yuxi, Wu. Zhongxian, Du. Xiaoyu, Yanbin Jiang, Beibei Ma, and Meihong Chi. 2022. The psychology of the internet fraud victimization of older adults: A systematic review. *Frontiers in Psychology* 13 : 912242. https://doi.org/10.3389/fpsyg.2022.912242.
Siporin, Max. 1980. Ecological systems theory in social work. *Journal of Sociology & Social Welfare* 7:507–532. https://doi.org/10.15453/0191-5096.1428.
Smith, Jonathan A. 1996. Beyond the divide between cognition and discourse: Using interpretative phenomenological analysis in health psychology. *Psychology & Health* 11:261–271. https://doi.org/10.1080/08870449608400256.
Smith, Jonathan A., Paul Flowers, and Michael Larkin. 2009. *Interpretative phenomenological analysis: Theory method and research*. London: SAGE.
Tinmaz, H., Y.-T. Lee, M. Fanea-Ivanovici, and H. Baber. 2022. A systematic review on digital literacy. *Smart Learning Environments* 9:21. https://doi.org/10.1186/s40561-022-00204-y.
Titus, R., and A.R. Gover. 2001. Personal fraud: The victims and the scams. *Crime Prevention Studies* 41: 54–77.
Tong, Peiru, and Irene Shidong An. 2023. Review of studies applying Bronfenbrenner's bioecological theory in international and intercultural education research. *Frontiers in Psychology* 14:1233925. https://doi.org/10.3389/fpsyg.2023.1233925.
US Department of Justice. 2023. *Annual Report to Congress on Department of Justice Activities to Combat Elder Fraud and Abuse.* October 18, 2023. https://www.justice.gov/elderjustice/media/1319976/dl?inline=. Accessed 4 June 2024.
Vandenbroucke, Guillaume and Heting Zhu. 2017. Aging and Wealth Inequality. *Economic Synopses, 2.* https://research.stlouisfed.org/publications/economic-synopses/2017/02/24/aging-and-wealth-inequality/. Accessed 14 June 2024.
Van Den Berg, H. 2005. Reanalyzing qualitative interviews from different angles: The risk of decontextualization and other problems of sharing qualitative data. *Forum Qualitative Sozialforschung Forum Qualitative Social Research*. https://doi.org/10.17169/fqs-6.1.499.
Van Deursen, A. J. A. M., and J. A. G. M. van Dijk. 2009. Using the internet: Skill related problems in users' online behavior. *Interacting with Computers* 21:393–402. https://doi.org/10.1016/j.intcom.2009.06.005.
Van Deursen, A. J. A. M., and J. A. G. M. van Dijk. 2011. Internet skills and the digital divide. *New Media & Society* 13:893–911. https://doi.org/10.1177/1461444810386774.
Van Wilsem, J. 2013. 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review* 29:168–178. https://doi.org/10.1093/esr/jcr053.
Vincenti, V. B., and R. K. Maurya. 2023. Relatives' understanding of perpetrators of elder family financial exploitation: A bioecological approach to understanding risk factors. *Victims and Offenders* 1–22. Advance online publication. https://doi.org/10.1080/15564886.2023.2265348
Whitty, M. T. 2019. Who can spot an online romance scam? *Journal of Financial Crime* 26:623–633.
Whitty, M. T., and T. Buchanan. 2016. The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice* 16:176–194. https://doi.org/10.1177/1748895815603773.
Williams, E. J., A. Beardmore, and A. N. Joinson. 2017. Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior* 72:412–421. https://doi.org/10.1016/j.chb.2017.03.002.
Worrilow, W.M., and R.D. Barraco. 2015. Physician Screening for Elder Abuse in the Emergency Department: A Literature Review. *Lehigh Valley Health Network Research Scholars Poster Presentation.* https://scholarlyworks.lvhn.org/research-scholars-posters/432/. Accessed 10 February 2024.