Security Journal (2025) 38:42
https://doi.org/10.1057/s41284-025-00482-4

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

Cybercrime against senior citizens: exploring ageism, ideal victimhood, and the pivotal role of socioeconomics

Suleman Lazarus[1,2,4] · **Peter Tickner**[3] · **Michael R. McGuire**[1]

Accepted: 20 May 2024

Abstract

We discuss cybercrimes against senior citizens from three standpoints: (a) online fraudsters often target senior citizens because of their age, which results in the propagation of ageism. Thus, we explicitly define ageism in the context of cybercrime, characterising it as the intentional targeting or prioritisation of senior citizens as potential victims of online fraud. (b) Senior citizens are vulnerable to online fraud schemes for physiological (e.g., cognitive decline), psychological (e.g., elevated fear of cybercrime), familial (e.g., insider fraud), and sociocultural (e.g., isolation) reasons. (c) Cybercrimes against older adults predominantly fall under the socioeconomic category driven by a common financial motive. We argue that ageism serves as a weapon used by online offenders to target older adults, whilst the concept of the ideal victim acts as society's shield in response to these reprehensible actions. This framework invites closer attention to how age-based targeting in cyberspace reproduces broader social, economic, and moral asymmetries. Future empirical studies are warranted to substantiate these claims beyond the theoretical realm.

Keywords Ageism and ageing · Elder abuse · Senior citizens · Vulnerabilities and risk factors · Ideal victims · Online fraud

✉ Suleman Lazarus
suleman.lazarus@gmail.com

[1] Department of Sociology, University of Surrey, Stag Hill, Guildford GU2 7XH, UK

[2] Mannheim Centre for Criminology, London School of Economics and Political Science (LSE), London WC2A 2AE, UK

[3] Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth PO1 2HY, UK

[4] Department of Sociology, University of the Western Cape, Cape Town, South Africa

Published online: 21 June 2025

Introduction

Ageism and fraud victimhood

> Why do financial scammers target seniors? Fraudsters and con artists go after older adults because they believe this population has plenty of money in the bank. But it is not just wealthy older [adults] who are targeted. Older adults with low incomes are also at risk for fraud (National Council on Aging 2023).

The intersection between cybercriminal activities targeting older adults and societal responses to such phenomena is found in Christie's (1986) seminal work, which delineates the attributes of the ideal victim. Christie argues that ideal victims are perceived by society as embodying specific traits aligning with societal norms of innocence, vulnerability, and lack of culpability, including physical frailty, moral rectitude, and the absence of involvement in the circumstances leading to their victimisation. Similar to previous scholarly works (e.g., Hock & Button 2023a; Loyens & Paraciani 2021), we leverage the "ideal victim" concept to elucidate the dynamics of online fraud victimisation. Specifically, we employ the term 'ideal victim' to illuminate the dynamics of scams[1] targeting older adults and the societal responses to such criminal acts. Whilst older adults may not exclusively constitute the primary targets of online scammers, their susceptibility to victimisation is pronounced because of inherent vulnerabilities such as physical frailty, cognitive decline, social isolation, limited Information Technology (IT) proficiency, and unfamiliarity with privacy and security threats. These factors not only render them ideal victims but also influence societal responses to their victimisation, including scholarly research. In addition to the idea of an ideal victim, we explore the concept of ageism.

Ageism stands out as one of the most profound challenges older adults face, stripping them of the self-respect afforded to others. Its impact is palpable across various spheres, with particular emphasis on its implications for older citizens' opportunities across multiple life domains. This study was motivated by three primary factors. (1) The socioeconomic dimension of cybercrime has emerged as a critical consideration. The prevalence of financially motivated "cyber-enabled crimes" targeting senior citizens delineates a distinct category within the spectrum of cybercrime. Whilst many crimes against seniors involve a financial motive, not all "cyber-enabled crimes" share this characteristic (cf. Lazarus et al. 2022). This underlines the significance of the socioeconomic dimension in classifying cybercrimes targeting older adults (cf. Ibrahim 2016). (2) Age-related risk factors and vulnerabilities are pivotal in shaping senior citizens' susceptibility to online fraudulent activities. Many age-related factors, including physiological, psychological, familial, and sociocultural factors, contribute to this heightened vulnerability. These factors intersect to create a unique set of

[1] In line with existing scholarship, this article uses the terms "scam" and "fraud," as well as "scammers" and "fraudsters," interchangeably. While "scam" is the more commonly used term among the media, financial institutions, and the general public, it is also adopted by organisations such as the Global Anti-Scam Alliance (GASA), Scamwatch, Scam Survivors, and Scam Baiters, all of which embed the term in their names. Within academic discourse, however, "fraud" tends to be favoured for its emphasis on the legal and financial dimensions of these offences (Lazarus et al. 2025).

circumstances that renders older adults particularly susceptible to online scams and fraud (Burton et al. 2022). (3) The intersection of ageism, ideal victims, and cybercrime further exacerbates the fraudsters' targeting of senior citizens. The amalgamation of ageist presumptions regarding older adults with identified risk factors amplifies their likelihood of becoming victims of fraudulent activities and their eligibility to become ideal victims. Ageism perpetuates stereotypes and biases that portray older adults as vulnerable and gullible, making them prime targets for cybercriminals seeking to exploit factors such as cognitive decline (cf. Butler 1969).

Ageism, as conceptualised by Butler (1969), represents a systemic form of discrimination characterised by prejudiced stereotypes and unjust treatment directed at individuals based solely on their advanced age. In this article, ageism encompasses discriminatory practices, preconceived notions, and biased attitudes towards individuals or groups based on age (Doron & Georgantzi 2018; Iversen et al. 2009; Manheim et al. 2022). Whilst ageism can affect both younger and older age groups, this study predominantly focussed on its implications for older adults. This article redefines ageism in the context of cybercrime as the deliberate targeting or prioritisation of seniors as potential victims of online fraud. We argue that ageism serves as a weapon used by online offenders to target older adults, whilst the concept of the ideal victim acts as society's shield in response to these reprehensible actions, underscoring the prevalence and scale of scams targeting the ageing population.

Ageing population trend

One of the most significant demographic challenges that governments face is population ageing. The global population of individuals aged 65 years or older is predicted to double from the 2021 figure of 761 million to more than 1.6 billion by 2050 (United Nations 2023). This trend was particularly pronounced for those aged 80 years and older. This worldwide phenomenon results from a demographic transition characterised by increased life expectancy and decreased family size (Doron & Georgantzi 2018; United Nations 2023).

This demographic shift brings forth a host of challenges, with one of the most pressing ones being the vulnerability of older individuals to various forms of fraud victimisation. As modern society increasingly relies on digital platforms and interconnected technologies, the ageing population is navigating an evolving technological landscape that intersects with age-related vulnerabilities. In conjunction with the University of Chicago, the American Association of Retired Persons (AARP) estimates from the Federal Bureau of Investigation (FBI) data for 2022 that the true level of losses for those aged 60 and over in the US is likely to be around $4.7 billion from internet crime alone (AARP 2023). Analysis of reported fraud losses to the US Federal Trade Commission (FTC) showed a reduced number of victims by each decade of age but a sharp rise in the average loss per victim for ages 70–79 and almost doubling again for those aged 80–89 (FTC 2023).

Although older people rarely report being victims of financial cybercrime, there is evidence that older online users are at increased risk (Burton et al. 2022). Research into the likelihood of elderly victims reporting financial and emotional mistreatment

suggests that only 66% of the financial abuse committed by strangers is likely to be reported. Where senior citizens are victims of family and friends, underreporting rises to 87.5% (Aciermo et al. 2020). Older adults are susceptible to financial losses due to various fraudulent activities, including tech assistance scams, reward schemes, sweepstakes, lotteries, and impersonation incidents involving family members and friends. Research has also demonstrated that when family members defraud older relatives, it can lead to severe consequences, such as the murder of elderly family members, often as an attempt to conceal criminal behaviour (Marquart & Thompson 2024). Analysis of internet crime complaints reported for 2023 estimates total losses to those aged 60 and over at $3.4 billion from 101,068 reported cases, double the losses reported for the age 50–59 bracket from 65,924 reported cases (FBI 2021). This study explicitly defines ageism within the context of cybercrime as the deliberate targeting or prioritisation of seniors as potential victims of online fraud enterprises. We argue that ageist assumptions of cybercriminals (fraudsters) merged with these risk factors heighten the likelihood of targeting individuals vulnerable to fraud. Hence, we carried out this conceptual work based on the following justifications.

I. To investigate the effects of ageism on older persons' online victimisation experiences, particularly in the context of cybercrime. By analysing the complex link between ageism and cybercrime victimisation, we aim to identify the elements that lead to older people's heightened vulnerability to cybercrime.
II. Ageism in the context of cybercrime is the purposeful targeting of older persons in online fraud operations, which has serious financial ramifications. The purpose was to shed light on the intricate connection between vulnerabilities and cybercrime, underscoring the importance of cybercrime categorisation and theorisation in understanding online victimisation amongst older adults.

The ambiguities of cyber-enabled crime as an analytic tool

The term cybercrime delineates illicit activities conducted through Information Communication Technology (ICT) and the Internet (Gordon & Ford 2006; Wall 2010; Yar & Steinmetz 2019). Whilst this term is frequently employed to encompass all illicit acts on the Internet, researchers, media, and security agencies often aggregate diverse digital offences under the broad umbrella of "cybercrime," neglecting their distinctive characteristics (Lazarus 2019, p. 18). Efforts to address this issue include differentiating between cyber-dependent and cyber-enabled crimes (McGuire & Dowling 2013). The former identifies digital offences that could occur without digital technology or networks, whilst the latter involves crimes that could be 'amplified' to some extent through networks. For instance, fraud accesses a broader audience through mass email campaigns. However, this binary classification limits a more comprehensive examination of the various axes of differentiation in cyberspace, such as gender differences (Lazarus 2019). This also obscures some of the deeper assumptions and motivations shared by cybercriminals. Specifically, the amalgamation of "cyber-enabled crimes" (McGuire & Dowling 2013) or "people-centric cybercrimes" (Gordon & Ford 2006) into a single category presents a

challenge in distinguishing between financially motivated cybercrimes like "online fraud" and psychologically driven offences such as "cyberbullying" (Ibrahim 2016; Lazarus 2019).

Therefore, contrary to the twofold classifications (i.e., the lens of "cyber-enabled crimes"), scholars have employed the Tripartite Cybercrime Framework (TCF) to establish clear boundaries between financially motivated cybercrimes (referred to as the socioeconomic category) and psychologically driven digital crimes (known as psychosocial cybercrime) (for a detailed examination of cybercrime categorisations, see Ibrahim 2016; Lazarus 2019; Lazarus et al. 2022). Whilst the TCF (Ibrahim 2016; Lazarus 2019) categorises cybercrimes into three primary motivational components (socioeconomic, psychological, and geopolitical), we utilise the distinction between socioeconomic and psychosocial cybercrime to spotlight that whilst most crimes against seniors are financially motivated. However, not all "cyber-enabled crimes" share this characteristic, thus emphasising the crucial socioeconomic dimension. Figure 1 below (adapted from Ibrahim 2016, p. 46) illustrates how the binary distinction typically functions, "highlighting issues with the interpretation of 'cyber-enabled crimes" (Lazarus et al. 2022, p. 381).

This binary model of cybercrime becomes more complex when discernible variations in motives, benefits, or losses experienced by the victim and offender in the phenomena of online revenge pornography and fraud are overlaid. These binary classifications of online criminal behaviour, as defined by Gordon and Ford (2006) and McGuire and Dowling (2013), fail to consider the significant impact of motivation, as some scholars have pointed out (e.g., Ibrahim 2016; Lazarus et al. 2022). This contradicts Rosch's (1978, p.28) principle of category formation, which emphasises

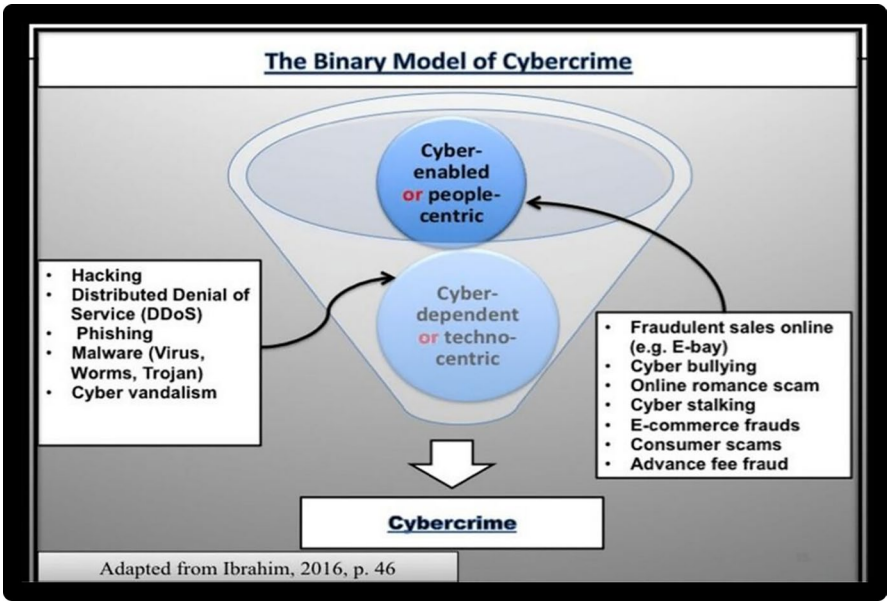

Fig. 1 The twofold classifications of cybercrime

the importance of acknowledging the influence of motivation whilst adhering to fundamental psychological categorisation principles:

> The task of category systems is to provide maximum information with the least cognitive effort [because] the perceived world comes as structured information rather than arbitrary attributes. Thus, maximum information with [the] least cognitive effort is achieved if categories map the perceived world structure as closely as possible. This condition can be achieved either by the mapping of categories to given attribute structures or by the definition or redefinition of attributes to render a given set of categories appropriately structured.

To address online elder abuse effectively, it is necessary to have a deeper understanding of the structure behind online victimisation. This study emphasises the importance of categorising cybercrimes more sensitively. It elucidates the analytical implications of homogeneity whilst underscoring the significance of categorising cybercrimes to understand ageism within criminal behaviour.

We explore the contention that older adults are more susceptible to socioeconomic cybercrime, particularly online fraud, owing to many factors contributing to their vulnerability. These factors include diminishing cognitive capacities associated with ageing, continually evolving tactics employed by cybercriminals, and intricate economic motives that drive their activities. Although some scholars have classified cybercrime (Gordon & Ford 2006; McGuire & Dowling 2013; Wall 2010), however, the Tripartite Cybercrime Framework (TCF) identifies three primary motivational drivers underlying cybercriminal activities (Ibrahim 2016; Lazarus 2019; Lazarus et al. 2022). Therefore, we acknowledge the TCF classifications that align with Rosch's (1978) principles of category formation, facilitating a nuanced recognition of socioeconomic factors relevant to discussions of scams against the ageing population.

Significance and centrality of socioeconomics

While the socioeconomic cybercrime involves the pursuit of financial gains through deceptive practices facilitated by computers or Internet technologies (Ibrahim 2016), this classification encompasses various illegal activities, such as Business Email Compromise (BEC) (Lazarus 2024), romance scams (Soares et al. 2025), copyright theft, and illegal downloads of digital content (Button et al. 2022, 2023; Hock & Button 2023b; Ibrahim 2016). Practices within this category include prevalence, impersonation, manipulation, counterfeiting, forgery, and fraudulent misrepresentation; notable examples include online romance and credit card fraud (Button et al. 2022; Lazarus et al. 2025). Online romance fraud is distinct in that it utilises romantic relationships to deceive victims into providing financial support, highlighting the fundamental socioeconomic nature of these crimes (Lazarus et al. 2023; Soares et al. 2025).

The value of the socioeconomic dimension of TCF becomes evident when we consider that crimes against seniors online have a predominantly financial

motivation (Ibrahim 2016; Lazarus 2019). This category encompasses cybercrimes driven by financial gain and executed through deceptive strategies that exploit individuals' economic resources and trust. Conversely, cyber-enabled crimes, the binary paradigm often used to assess cybercrime against seniors, can create the misconception that these crimes result solely from technological advancements (Lazarus 2019). Whilst cyber-enabled crimes encompass various offences, including revenge pornography and cyber rape, cybercrime against seniors finds its primary foundation in socioeconomics (Ibrahim 2016; Lazarus 2019).

Based on the above remarks, the significance of our argument lies in its elucidation of the distinctiveness of cybercrimes against senior citizens within the broader category of cyber-enabled offences. Our argument emphasises that cybercrime against senior citizens forms a unique category. This identification is crucial for understanding the specific nature of the threats older individuals face online, setting them apart from the broader spectrum of so-called 'cyber-enabled crimes'. Recognising heterogeneity within the broader category of cyber-enabled crimes is vital for refining our understanding of cyber threats and tailoring preventive measures to address the specific vulnerabilities of senior citizens (Lazarus 2019). Based on the above remarks, we posit that online perpetrators utilise ageism as a means to prey on older individuals, whilst the construct of the ideal victim serves as society's protective barrier in reaction to these condemnable acts. We now highlight how age-related risk factors, such as psychological, familial, social, and physiological factors, and ageism assumptions of cybercriminals make senior citizens more susceptible to fraudulent schemes.

Ageism, socioeconomics, theories, and vulnerabilities

A poem: ageism and online fraud victimhood

Life's mysteries enthral as we age and grey.
As we shadow away, we hear the twilight's dance.
Within the shadows, masquerades waltz and sway.

Cognitive decline, come what may,
Loneliness, the shadows of lost romance.
Cyber vulnerability lurks, a complex game at bay.

As we age and grey, keys misplaced, we slip and fall,
In the chaos, scammers clamber into the banking hall.
To help us, to hold us, to guide us, to feed us.

As we age and grey, life's mysteries enthral us,
The fruits we plucked in youthful, vibrant sway,
Now pilfered by the night, fraudsters laugh, "It is a game, play!".

We present an original poem above that radiates from the themes of this article. As highlighted by Longo (2015, p. 56), whilst this approach "might appear strange" to some contemporary sociologists, the historical precedence of utilising literary works to gain deeper insights into human reality is undeniable. Whilst this type of creative intervention, blending poetry in research reports, is gaining traction in the social sciences and humanities (e.g., Lazarus 2021; Parsons & Pinkerton 2022), our approach builds upon the groundwork laid by early sociologists (cf. Farrell 1954; Znaniecki 1934). These scholars (Farrell, 1954; Znaniecki, 1934) advocated subjecting literary sources such as poetry to sociological analysis. We align ourselves with these early scholars, sharpening the sociological eyes of our discussions of age-related risk factors.

Age-related risk factors and vulnerabilities

Ageist assumptions of fraudsters, combined with age-related risk factors, make senior citizens more susceptible to fraudulent schemes. "A risk factor," as articulated by Kazdin et al. (1997, p. 377), is defined as "a characteristic, experience, or event that, if present, is associated with an increase in the probability (risk) of a particular outcome over the base rate of the outcome in the general (unexposed) population." This suggests that whilst risk factors are associated with age-linked vulnerabilities, they do not have a cause-and-effect relationship: they cannot be assessed in isolation, given their dynamic interaction with protective factors (cf. Kazdin et al. 1997). Therefore, we concluded that these risk factors were not deterministic. Conversely, protective factors such as a support network only moderate the potential consequences of risks and do not share a direct association with age-related vulnerabilities. We now discuss these risk factors.

Susceptibility to cybercrime is intricately woven into an individual's capacity to navigate life changes, shaping vulnerability and resilience dynamics (Castañeda et al. 2021). In the context of older individuals, recognising the nuanced relationship between vulnerability and resilience is crucial. Researchers underscore that certain vulnerable groups, particularly older individuals, may not fully harness the benefits of Information Communication Technologies (ICTs) because of limited awareness of ICTs or concerns about risks (Castańeda et al. 2021). "Limited awareness" refers to limited awareness of ICT and associated risks. By acknowledging and addressing the distinctive challenges that older adults face in navigating the digital realm, we can empower senior citizens, ideal victims, and participate whilst preserving privacy and self-worth.

As the global population ages, with the proportion of individuals over 65 doubling from less than 9% in the 1960s to 18% in 2021 (United Nations 2023), criminal fraud cases targeting seniors are increasing. Fraud and deception aimed at this demographic pose a significant social challenge on a global scale (Wen et al. 2022). A US-based review spanning 25 years revealed that 5.4% of cognitively intact elders fall victim to financial scams annually (Burnes et al. 2017). Data from the US Federal Trade Commission (FTC 2023) indicate that social media is the primary first contact for fraudulent victims aged 60–69, whilst phone calls initiate contact for

those aged 70 and above. Financial losses due to fraud for individuals aged 80 and over were nearly three times as high as in other age groups, emphasising the severity of the issue. Many of the top ten financial scams targeting seniors in 2023 utilised ICTs, including online shopping scams, tech support scams, lottery scams, often leveraging the persuasion of credit card usage.

As individuals age, they encounter an array of vulnerabilities that contribute to susceptibility to fraudulent schemes (Chen et al. 2025). Although scams can target anyone, seniors are especially susceptible (Conway & Kirk-Wade 2021). Age-related susceptibilities include cognitive decline, diminished decision-making abilities, financial instability, and an increased tendency to trust others. These vulnerabilities significantly heighten susceptibility to cybercrime, particularly in the context of socioeconomic cybercrime (Castañeda et al. 2021). The interplay of age-related vulnerabilities aligns with the socioeconomic dimension of TCF, illuminating the economic motivations that cybercriminals exploit when targeting older adults. Whilst a deep understanding of these vulnerabilities is paramount, these risk factors include social isolation, health vulnerabilities, memory loss, wealth, limited cybersecurity skills or awareness, and societal attitudes (Burton et al. 2022; Shao et al. 2019).

Cognitive decline

The natural ageing process intertwines with cognitive decline, affecting various cognitive domains such as memory, reasoning, and problem-solving abilities. This age-associated cognitive deterioration diminishes an individual's capacity to identify and respond appropriately to indicators of fraudulent activities (Burton et al. 2022; Han et al. 2015, 2016; James et al. 2014). Furthermore, cognitive decline can lead to older adults seeking emotional substitutes for the loss of a partner or reduced social life, triggering feelings of isolation and increasing their risk of falling victim to fraud (Wen et al. 2022). Cybercriminals exploit cognitive decline by crafting scams designed to confound older adults and coerce them into decisions that imperil their financial security.

The ageing process reduces the ability to make complex decisions, rendering older adults more susceptible to the persuasive tactics employed by cybercriminals. Manipulative strategies such as high-pressure sales techniques or disseminating fear-inducing messages exploit this vulnerability and may result in older adults becoming victims of fraud. Comparative studies (e.g., Judges et al. 2017) have demonstrated that older adults with significant cognitive decline are more likely to become victims of scams and fraud than those with less severe cognitive decline. As people age, they become more incentivised by positive messages (Burton et al. 2022; Kircanski et al., 2018). Thus, with cognitive decline, individuals can be attracted to scams and cybercrimes, offering rewards such as health cures, lottery prizes, or short-term gratification (Kircanski et al. 2018). We contend that whilst ageism functions as a tool wielded by cybercriminals to victimise older adults, the notion of the perfect victim serves as society's defence mechanism against such deplorable behaviour. We argue that ageist assumptions

of cybercriminals merged with these age-related risk factors heightened the likelihood of targeting individuals vulnerable to fraud.

Three distinct forms of cognitive decline

We identified three distinct forms of cognitive decline, each influencing seniors' susceptibility to cybercrime. First, gradual cognitive decline is observed in mentally alert individuals in old age. Second, rapid decline affects individuals with dementia or brain-related diseases. Lastly, sudden cognitive decline in otherwise cognitively alert individuals is triggered by traumatic events, such as the death of a life partner, loss of independence, or major financial setbacks. Additional risk factors such as social isolation or mental illness/depression can accelerate the impact of these forms.

- *Gradual cognitive decline* the slow decline of mental alerts exposes people to the risk of cybercrime. They may recognise the threat but forget to take protective measures or inadvertently make mistakes online (Hans et al. 2016).
- *Rapid cognitive decline* (*dementia*) cognitive impairment from any degree of dementia affects the judgment of the individual and increases the likelihood that those without a strong care and support network around them will fall victim to cyber-enabled crimes (Judges et al. 2017; Xing et al. 2020).
- *Sudden cognitive decline* individuals experiencing sudden cognitive decline become more vulnerable to romance fraud and similar cybercrimes following a traumatic event (Xing et al. 2020).

Cognitive decline and socioeconomics

Whilst cognitive decline is prevalent amongst very senior citizens and individuals experiencing age-related conditions such as Alzheimer's and dementia (Boyle et al. 2019), cognitively intact older adults can fall prey to cybercrime as they age. Although the extent of cognitive decline varies amongst individuals (Ren et al. 2023; 2024), research suggests that regardless of their cognitive status, ageing adults are susceptible to online scams (Boyle et al. 2019; Shao et al. 2019). Individuals with dementia are at a greater risk of financial abuse scams and cybercrimes triggered by the actions of relatives or caregivers using their internet access. Those who have maintained independence in old age may also suffer from cognitive decline that goes undetected or undiagnosed until it is too late to protect them from becoming victims of scams or cybercrimes. Healthcare professionals are often at the frontline in discovering that senior citizens are being financially abused, but without adequate training, they may not know how best to prevent such abuse (Burnes et al. 2017; 2019).

Financial stability

The financial stability that often comes with age can also make older adults attractive targets for cybercriminals (Burton et al. 2022). Older populations may possess substantial assets and relative wealth, making them alluring prospects for various forms of financial fraud (see Fig. 2). Cybercriminals prey on them by creating scams that promise substantial returns or security breaches that require immediate action (Burton et al. 2022).

In 2017, three federal entities–the Consumer Financial Protection Bureau, the U.S. Department of Treasury, and the Financial Crimes Enforcement Network (FinCEN)—concluded that financial exploitation is the most common form of elder.

Abuse in the United States (Rebovich & Corbo 2022). The reported financial loss from cybercrime to US citizens rose from $1.418 billion in 2017 to $1.7816 billion in 2018, with seniors accounting for 24% of the victims and 34% of the losses (IC3 2019). The crux of the issue for victims over 60 years of age, who often no longer participate in the workforce, is that they usually have neither the means nor the opportunity to repair their financial situation after victimisation (cf. Button et al. 2024). Senior citizens are most likely to have fixed incomes or limited employment opportunities, where the consequences of falling victim to scams or cyber-enabled fraud can be financially and personally devastating, resulting in a substantial reduction in independence and well-being (Button et al. 2024; Han et al. 2016).

In the context of financial stability as a risk factor, the corollary of financial instability can also be a risk factor for senior citizens. Senior citizens with relatively low funds can perversely be more tempted to try riskier schemes that promise unrealistically high dividends to boost their income. For cybercriminals, this is a potential gold mine enabling them to target those with limited funds, as they are more likely to invest those funds in a ‘get rich quick’ scam. For example, a survey by Kasim et al. (2023) indicated that retirees with limited funds tend to seek riskier investments. Cybercriminals exploit the psychological vulnerability of greed, often targeting elderly individuals who perceive significant opportunities to invest in fake businesses (Rebovich & Corbo 2022). It is not always about greed. It may instead reflect a desire to engage in altruistic or socially meaningful pursuits. Cybercriminals may rationalise their schemes to elderly victims by convincing them that a portion of their imagined financial gains will be allocated to bogus charities or purportedly noble causes (Rebovich & Corbo 2022).

The psychological impact on the well-being of older citizens who become victims of cybercrimes can be as or more devastating than the impact of financial loss alone on cybercrime, leading to significant cognitive decline, increased fear of abuse, feelings of shame and guilt, depression, and in extreme cases, suicide (e.g., Piterova 2020). The financial stability of senior citizens can be eliminated by scams and cybercrimes, causing some individuals to lose their life savings and remove their ability to meet the costs of day-to-day living because many are on fixed or declining incomes. Crimes against senior citizens, especially economic scams, increased during the COVID-19 pandemic (Teaster et al. 2023). Research into reported crimes in

the UK identified that senior citizens were more likely to become repeat victims of cybercrimes (Sikra et al. 2023).

Social isolation

Empirical evidence has substantiated that loneliness in older adults heightens their susceptibility to online fraud (Philips 2017; Wen et al. 2022). This conclusion was drawn from both qualitative (Philips 2017) and quantitative (Wen et al. 2022) research. Seniors who feel lonely and struggle to interact socially or who have medical needs in old age are more likely to become victims of fraud (Xing et al. 2020). Older adults' restricted ability to engage in peer learning networks exacerbates their vulnerability in the digital realm. Social isolation imposes substantial challenges, effectively curtailing their access to collective wisdom and hampering their capacity to discern the quality of advice related to online security (Nicholson et al. 2019; Roberts et al. 2013).

Contrary to common perceptions, social isolation leading to loneliness is not inherently more prevalent amongst senior citizens than other age groups, nor is it more likely to increase with age (ONS 2023). However, age-induced isolation may vary across cultures, as older adults in non-Western societies often reside with their children and grandchildren more frequently than in Western societies. Additionally, Redmile (2019) suggested that individuals from collectivist cultures, such as Vietnam, Brazil, and India, may have distinct cybersecurity threat models compared to those from individualist cultures, such as Australia, the United States, and the United Kingdom. Nevertheless, when senior citizens experience social isolation and loneliness, their susceptibility to cybercrime victimisation may increase.

According to disengagement theory (Cumming 1964), as individuals age, they tend to withdraw from social engagement. Adams (2004) found that individuals over 75 were more likely to disengage from social interactions, potentially leading to decreased digital awareness and reduced interaction with social media platforms. An analysis conducted in the US on seniors who reported financial abuse in 2023 revealed that, within the 60–69 age bracket, fraudsters most commonly contacted victims through social media, followed by websites or apps, with phone calls being the third most common method. However, for seniors aged ≥ 70 years, fraudsters predominantly used phone calls as their primary contact method, followed by email (FTC 2023).

Senior citizens who do not grow up with the current technology may feel alienated or struggle to understand its purpose (Burton et al. 2022). Although the next generation of seniors is likely to be more technologically aware than their predecessors, technological advancements will continue, potentially perpetuating cycles of disengagement. On the other hand, Gerotascendence theory (Tornstam 1997) suggests that individuals may transition from materialistic pursuits to a more holistic view of life as they age. This shift may create a psychological barrier between cybercriminals and their intended victims, as some seniors may choose not to engage in online scams or financial threats. However, as noted by Tornstam (1997), not all seniors mature into Gerotranscendence, and those who do not may be at greater

risk of victimisation by cybercriminals. Disengagement theory and Gerotascendence theory offer valuable insights into the social dynamics of ageing.

Disengagement theory provides insights into withdrawal from social engagement commonly observed in older adults, which can contribute to increased vulnerability to cybercrime. On the other hand, Gerotascendence theory offers a contrasting perspective. It suggests that some older adults may transition to a more holistic and less materialistic view of life, potentially influencing their susceptibility to cyber threats. Disengagement theory focuses on social disengagement as individuals age, emphasising the potential consequences of digital awareness and susceptibility to cybercrime. In contrast, Gerotascendence theory highlights the psychological and existential aspects of ageing, suggesting that shifts in worldview may influence older adults' interactions with technology and cyber threats. Researchers and practitioners can develop tailored interventions by understanding different pathways to cybercrime vulnerability and promoting protective factors associated with social engagement, technological literacy, and existential fulfilment.

Increased trust in others and financial abuse

A significant proportion of older adults live in a period characterised by higher levels of trust in societal institutions and individuals, as highlighted by the United Nations (2023) and Chen et al. (2025). Trust in others can expose them to potential exploitation by cybercriminals, who portray themselves as reliable and trustworthy figures. According to systematic reviews of romance scam literature published over the past two decades (Bilz et al. 2023; Lazarus et al. 2023), and convicted case files of romance fraudsters (Soares & Lazarus 2024; Soares et al. 2025), malevolent actors exploit trust by forming deceptive online relationships to persuade individuals, including older adults, to disclose sensitive personal or financial information.

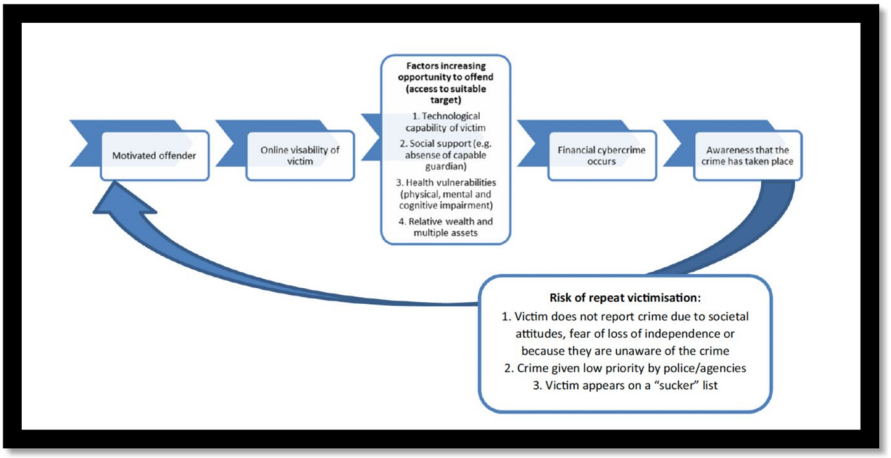

Fig. 2 Factors increasing opportunity for defrauding ageing population. Figure modified from Burton et al. (2022, p. 3)

The willingness to trust others becomes vulnerable when navigating the digital landscape.

Exploitation of older adults is not restricted to external threat actors. In some distressing instances, individuals who should serve as protective shields, namely, families and friends, betray trust (Marquart & Thompson 2024). Research (2024) indicated that they manipulated and defrauded senior citizens (e.g., Aciermo et al. 2020; Marquart & Thompson 2024). In such cases, the motivation behind these crimes is unequivocally financial. A study on the prevalence of emotional, physical, sexual, and financial abuse of senior citizens in the US found that 5.2% of senior citizens had suffered financial abuse by a family member in the past year (Acierno et al. 2020). Similarly, Marquart and Thompson's (2024) research in the United States revealed that crimes involving close relatives, such as grandchildren, can escalate to the murder of elderly family members. The probability of abuse was notably elevated amongst individuals who experienced greater social isolation, thereby increasing their susceptibility to becoming victims of cybercrime (cf. Acierno et al. 2020; Marquart & Thompson 2024).

Based on the above, we contend that senior citizens are at high risk of being negatively impacted by various factors. Criminals may target senior citizens to exploit their financial resources and assets, as shown in Fig. 2, which highlights the financial motivation behind crimes against this cohort. The financial aspects of these crimes, their underlying motives, and their impact on the financial security of older adults are areas that require further research and understanding. Although financially motivated cyber-enabled crimes against seniors are common, not all 'cyber-enabled' crimes are committed for financial gain (Lazarus 2019). The TCF demonstrates that not all categories of cybercrime are financially motivated, highlighting the importance of understanding the utilitarian value of its three-way dimensions (Ibrahim 2016; Lazarus 2019; Lazarus et al. 2022). Therefore, it is evident that the socioeconomic dimension plays a significant role in the unifying factor whereby cybercrimes against seniors are predominantly financially motivated. This further emphasises the need to understand this specific dimension of cybercrime and its impact on older adults. Senior citizens face additional challenges in the digital world besides psychological, familial, and physiological factors.

Limited understanding of digital privacy and security

Limited digital privacy and security knowledge and belief in online threats increase senior citizens' susceptibility to online fraud. These factors can lead older adults to forgo essential security measures (Burton et al. 2022; Nicholson et al. 2019; Roberts et al. 2013), and non-inclusive technology designs can exacerbate them (cf. Köttl et al. 2021). Fraudsters take advantage of older adults' limited knowledge of computer technology and their technological naivete, which could make them more susceptible to becoming victims of online scams (Burton et al. 2022; Nicholson et al. 2019). A significant number of cases targeted elderly victims' lack of awareness of the instant nature of bank transfers or the existence

of fake websites masquerading as genuine. Cybercriminals would switch email addresses, aliases, and phone numbers to confuse and confound elderly victims (Lazarus 2024; Rebovich & Corbo 2022).

Consider a scenario in which a senior citizen receives a call that appears to be from their bank, urgently requesting action to prevent unauthorised account access. Owing to their elevated fear of cybercrimes, they may respond to this seemingly urgent request without verifying the call's authenticity. Even if they were alert enough to call the number on the bank's website to ensure that it was genuine, they may not be aware that the fraudster could stay on the line, and the victim would end up calling the fraudster, not the bank, in their haste to protect funds. Cybercriminals are highly persistent once they establish contact. Less ICT-aware senior citizens find it difficult to see through the scammer's web of deceit and pressure put on them to respond urgently. When the fear factor drives a cybercriminal victim, their emotional state will likely impair their decision-making and judgment.

The Office for National Statistics (ONS) surveyed crime in the UK up to March 2023 and revealed that 6.3% of all adults had been victims of fraud, of which 2.8% were cyber-enabled (ONS 2023). Amongst adults aged 65–74, the percentage of fraud victims decreased to 5.8%, with 2% experiencing cyber-enabled fraud. For individuals aged 75 and older, the incidence further declined to 4.4% for all types of fraud and 1.4% for cyber-enabled crimes (ONS 2023). Whilst this could be attributed to an elevated fear of crime, resulting in less Internet usage, it could also reflect a fear of admitting having been a victim of crime or a lack of awareness of having been a victim at all. Certainly, financial motivation is a common denominator in cybercrimes targeting seniors (Burton et al. 2022). However, this is not the case for all cyber-enabled crimes, highlighting the pivotal role of the socioeconomic dimension within the Tripartite Cybercrime Framework (TCF) (Lazarus 2019).

Elevated fear of cybercrime

Fear can lead to seniors' avoidance of online services and the neglect of necessary security measures, rendering them more susceptible to various cyber manipulations. Heightened fear of digital crimes, combined with their belief in online threats, can lead older adults to forgo essential security measures and, in some cases, to avoid online services (Nicholson et al. 2019; Roberts et al. 2013). Cybercriminals prey on the fear of cybercrime either by calling the victims to tell them that they have allowed their computer to become infected and need to download software to protect themselves or by causing a pop-up message to tell the victim their computer has become infected. The fear generated by these approaches can cause the elderly victim to allow cybercriminals access to their computer in the belief that they are preventing a virus when, in fact, they are downloading malicious software to help the criminal access their financial records. Again, whilst financial motivation is a common denominator in cybercrimes targeting seniors, this is not the case for all cyber-enabled crimes, highlighting the pivotal role of socioeconomic dimension within the Tripartite Cybercrime Framework (TCF).

Internet use confidence

Perceived vulnerability to cybercrimes amongst seniors significantly contributes to a heightened fear of falling victim to fraudulent activities (Karagiannopoulos et al. 2021; Nicholson et al. 2019). Confidence in Internet use varies significantly amongst older adults, presenting challenges, particularly for regular Internet users. One common issue is a lack of confidence in seeking security information or resolving security and technical issues (Nicholson et al. 2019). This lack of confidence fosters a sense of vulnerability, and language barriers can exacerbate this challenge, making older Internet users less adept at navigating the digital landscape (Karagiannopoulos et al. 2021; Nicholson et al. 2019).

For example, consider an older adult who frequently uses the Internet for communication and shopping. They encounter a pop-up message on a shopping website, seemingly requesting an update on their payment information. Owing to their limited confidence in discerning security-related issues, they might proceed with the update, inadvertently falling victim to a phishing scam. The inability of senior citizens to differentiate between legitimate and fraudulent security alerts can have significant financial implications. Ageist assumptions by both fraudsters and Internet service providers, including providers of antiviral technologies, enhance the risks to seniors. We assert that online offenders employ ageism to target older adults, whereas the concept of the ideal victim acts as a society's safeguard in response to these reprehensible deeds. Drawing on Fig. 2, we also contend that these risk factors disproportionately and adversely affect seniors, leading to online fraud.

Lack of reporting mechanisms awareness

Similar to other age groups, a substantial portion of senior citizens lack awareness of the mechanisms for reporting cybercrimes, leading to significant underreporting. This emphasises the need for tailored reporting materials and peer support networks to cater to their needs (Burton et al. 2022; Nicholson & McGlasson 2020). For example, consider an older adult who receives a phishing email attempt. In this scenario, they may not know how to report or understand the necessity. Consequently, they might delete or ignore the email, inadvertently neglecting the opportunity to prevent others from falling for the same scam. These types of actions imply that seniors are less likely to consider cybersecurity implications (cf. Nicholson et al. 2019).

Summary

Vulnerabilities, ageism, and the role of socioeconomics

This section summarises the key arguments that help us to understand cybercrime against senior citizens.[2] These arguments focus on the socioeconomic dimension

[2] Some of the content in this section will also be included in the "Originality and Implications" section, as both are integral components of the summary section.

of cybercrime, age-related risk factors and vulnerabilities, and the intersection of ageism and cybercrime. Financially motivated "cyber-enabled crimes" targeting senior citizens (e.g., online fraud) are prevalent and form a distinct category within the spectrum of cybercrime, unlike other forms of "cyber-enabled crimes" (e.g., revenge pornography). However, not all "cyber-enabled crimes" are financially motivated (Ibrahim 2016; Lazarus 2019), highlighting the essential socioeconomic dimension in classifying cybercrimes. Furthermore, various age-related factors spanning physiological, psychological, familial, and sociocultural domains contribute to the heightened susceptibility of seniors to fraudulent online activities. The amalgamation of ageist presumptions concerning cybercriminals, particularly fraudsters, with the identified risk factors amplifies the likelihood of targeting senior citizens for fraudulent activities. The interplay between these forces necessitates a nuanced understanding of how societal biases intersect with cybersecurity threats, especially concerning senior citizens' victimisation.

Moreover, the vulnerabilities associated with ageing can have severe implications for seniors who have become victims of fraudulent schemes. Cybercriminals are skilled at creating schemes that take advantage of cognitive decline, reduced decision-making abilities, financial instability, and increased trust that older adults often place in others. These schemes, ranging from investment fraud to romance scams, rely on vulnerabilities to deceive and defraud older people. Acknowledging the financial incentives behind cybercrime, the TCF's socioeconomic category can offer valuable insights into the relationship between financial incentives and the vulnerabilities associated with ageing, as opposed to the "cyber-enabled crime" category illustrated in Fig. 1. Our research aims to explore the connection between the socioeconomic aspect of the Tripartite Cybercrime Framework (TCF) and the economic incentives that drive fraud perpetrators. This alignment highlights the practical implications for policy recommendations. The threat of various socioeconomic types of cybercrime against older adults is multifaceted, and we argue that ageist assumptions combined with identified risk factors increase the likelihood of targeting individuals vulnerable to fraud. By acknowledging the inherent connection between financial motivations and susceptibilities linked to ageing, we can develop targeted countermeasures to protect senior citizens from the intricate web of cybercrimes.

Originality and implications

1. This article constitutes a conceptual exploration of elder abuse and online fraud. It highlights the integration of the socioeconomic facet within the Tripartite Cybercrime Framework (TCF) to scrutinise the diverse vulnerabilities senior citizens encounter in the digital landscape. In doing so, it advances our understanding of the intricate challenges senior citizens face in the digital domain, emphasising pivotal factors such as cognitive decline, social isolation, trust, digital literacy, fear, and reporting awareness that mould their susceptibility to cybercrimes. Our approach weaves together age-related risk factors scattered in the existing litera-

ture with an original poem interwoven with insights from socioeconomic cybercrime types. This amalgamation of insights sheds light on online crimes against seniors.

2. We strategically employ the socioeconomic lens of the TCF to spotlight the need to differentiate financially motivated cybercrimes against senior citizens from other cyber-enabled offences. The article underlines a commonality amongst cybercrimes targeting senior citizens: the dual characteristics of being financially motivated and cyber-enabled, as illustrated in Fig. 1. However, this emphasises the nuanced distinction that not all cyber-enabled crimes share this financial motivation. This refined perspective accentuates the pertinence of the socioeconomic dimension, shedding light on the fact that online crimes against seniors inherently possess financial motivation, mirroring the financial motivation embedded in all socioeconomic cybercrimes.
3. We pioneered the redefinition of ageism to encompass the deliberate targeting or prioritisation of seniors by offenders for online fraud victimisation. Our research sets itself apart by emphasising the intersection of ageism and cybercrime. This contention posits that the amalgamation of ageist preconceptions of cybercriminals with these identified risk factors heightens the proclivity to target vulnerable individuals for fraudulent activities. We offer insights into developing more effective measures to protect vulnerable populations, particularly seniors, from online threats. We establish a foundation for empirical research that recognises age as a crucial factor in the evolving landscape of cybercrime.

These three layers of findings have profound implications for creating targeted educational initiatives, support systems, policies, and awareness programmes. These measures are essential for reducing the risks faced by senior citizens online and for ensuring their financial security. Whilst our research provides a new perspective, it lays the foundation for proactive measures to safeguard well-being.

Conclusion

We discussed the pivotal role of the socioeconomic category of cybercrime against senior citizens from a conceptual lens encompassing interconnected ideas and principles. These guide a deeper understanding of this crime type and demographic in an era when the pace of population ageing is accelerating more rapidly than ever before. We identified signs of ageist targeting by cybercriminals in developed economies with the highest volumes of internet-based crime. We discuss the importance of socioeconomic classification in understanding the landscape of cybercrime against senior citizens. The argument is presented along three key dimensions: (a) whilst digital crimes against seniors are predominantly financially motivated, financial motivation is not universal to all cyber-enabled crimes directed at this demographic. (b) On the other hand, the significance of the socioeconomic facet becomes explicitly evident by recognising that internet-based crimes against seniors are predominantly financially motivated and that socioeconomic cybercrimes inherently

share this common financial motivation. (c) The analysis revealed that online fraud against senior citizens results from various physiological, psychological, familial, and social vulnerabilities amongst seniors. Therefore, this demographic becomes particularly susceptible to cybercrime perils.

This study uncovers a complex interplay between ageism, the notion of the ideal victim, socioeconomic cybercrime, and multifaceted vulnerabilities. These findings contribute to a deeper understanding of senior citizens' challenges in the digital age. We argue that ageism serves as a weapon used by online offenders to target older adults, whilst the concept of the ideal victim acts as society's shield in response to these reprehensible actions. We call for deeper examination of how digital ageism intersects with structural disparities across society. We also highlight the need for tailored interventions and safeguards to protect this vulnerable population from the constantly evolving cybercrime landscape. Future empirical studies are needed to substantiate these claims beyond the theoretical realm.

Data availability Not applicable.

Declarations

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

References

AARP (2023). The scope of elder financial exploitation: What it costs victims. Retrieved: https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/scope-elder-financial-exploitation.html#:~:text=The%20true%20cost%20of%20EFE,for%20which%20consumers%20ultimately%20pay.

Acierno, R., M. Steedley, M. A. Hernandez-Tejada, G. Frook, J. Watkins, and W. Muzzy. 2020. Relevance of perpetrator identity to reporting elder financial and emotional mistreatment. *Journal of Applied Gerontology* 39 (2): 221–225. https://doi.org/10.1177/0733464818771208.

Adams, K. B. 2004. Changing investment in activities and interests in elders' lives: Theory and measurement. *The International Journal of Aging and Human Development* 58 (2): 87–108. https://doi.org/10.2190/0UQ0-7D8X-XVVU-TF7X.

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 (6): 773–788. https://doi.org/10.1093/iwc/iwad048.

Boyle, P. A., L. Yu, S. E. Leurgans, R. S. Wilson, R. Brookmeyer, J. A. Schneider, and D. A. Bennett. 2019. Attributable risk of Alzheimer's dementia attributed to age-related neuropathologies. *Annals of Neurology* 85 (1): 114–124. https://doi.org/10.1002/ana.25380.

Burnes, D., R. Acierno, and M. Hernandez-Tejada. 2019. Help-seeking among victims of elder abuse: Findings from the National Elder Mistreatment Study. *The Journals of Gerontology: Series B* 74 (5): 891–896. https://doi.org/10.1093/geronb/gby122.

Burnes, D., K. Pillemer, and M. S. Lachs. 2017. Elder abuse severity: A critical but understudied dimension of victimization for clinicians and researchers. *The Gerontologist* 57 (4): 745–756. https://doi.org/10.1093/geront/gnv688.

Burton, A., C. Cooper, A. Dar, L. Mathews, and K. Tripathi. 2022. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology* 159 : 111678. https://doi.org/10.1016/j.exger.2021.111678.

Butler, R. N. 1969. Age-ism: Another form of bigotry. *The Gerontologist* 9 (4): 243–246.

Button, M., B. Hock, and D. Shepherd. 2022. *Economic crime: From conception to response*, 1st ed. London: Routledge.

Button, M., B. Hock, D. Shepherd, and P. Gilmour. 2023. Understanding the rise of fraud in England and Wales through field theory: Blip or flip? *Journal of Economic Criminology* 1 : 100012. https://doi.org/10.1016/j.jeconc.2023.100012.

Button, M., V. Karagiannopoulos, J. Lee, J. B. Suh, and J. Jung. 2024. 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.

Castañeda, A., Matheus, A., Klimczuk, A., Berti Suman, A., Duerinckx, A., Pavlakis, C., …& Woods, T. (2021). ICTs, data and vulnerable people: a guide for citizens, retrieved: https://www.econstor.eu/bitstream/10419/243095/1/ICTs-data-and-vulnerable-people-a-guide-for-citizens.pdf

Chen, H., M. He, and L. Peng. 2025. Understanding online shopping fraud among Chinese elderly: Extending routine activity theory in the online context. *Telematics and Informatics* 96: 102208. https://doi.org/10.1016/j.tele.2024.102208.

Christie, N. 1986. The ideal victim. In *From crime policy to victim policy*, ed. E. A. Fattah, 17–30. Palgrave Macmillan.

Conway, L. & Kirk-Wade, E. (2021). Protecting consumers from online scams. Retrieved: https://researchbriefings.files.parliament.uk/documents/CDP-2021-0064/CDP-2021-0064.pdf

Cumming, M. E. 1964. New thoughts on the theory of disengagement. In *New thoughts on old age*, ed. R. Kastenbaum. Berlin: Springer.

Doron, I. I., and N. Georgantzi. 2018. *Ageing, ageism and the law: European perspectives on the rights of older persons*. Cheltenham: Edward Elgar Publishing.

Farrell, J. T. 1954. Some observation on literature and sociology. In *Reflections at fifty and other essays*, ed. James T. Farrell, 142–155. New York: Vanguard Press.

FBI. (2021). Elder Fraud Report 2021, retrieved from: https://www.justice.gov/file/1523276/download (accessed 11/08/2023).

FTC. (2023), FTC consumer sentinel network. Retrieved: https://www.ftc.gov/enforcement/consumer-sentinel-network

Gordon, S., and R. Ford. 2006. On the definition and classification of cybercrime. *Journal in Computer Virology* 2 (1): 13. https://doi.org/10.1007/s11416-006-0015-z.

Han, S. D., P. A. Boyle, B. D. James, L. Yu, and D. A. Bennett. 2015. Poorer financial and health literacy among community-dwelling older adults with mild cognitive impairment. *Journal of Aging and Health* 27 (6): 1105–1117. https://doi.org/10.1177/0898264315577780.

Han, S. D., P. A. Boyle, B. D. James, L. Yu, and D. A. Bennett. 2016. Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease* 49 (3): 845–851.

Han, S. D., P. A. Boyle, K. Arfanakis, D. Fleischman, L. Yu, B. D. James, and D. A. Bennett. 2016. Financial literacy is associated with white matter integrity in old age. *Neuroimage* 130: 223–229. https://doi.org/10.1016/j.neuroimage.2016.02.030.

Hock, B., and M. Button. 2023a. Non-ideal victims or offenders? The curious case of pyramid scheme participants. *Victims and Offenders*. https://doi.org/10.1080/15564886.2023.2186996.

Hock, B., and M. Button. 2023b. Why do people join pyramid schemes? *Journal of Financial Crime* 30 (5): 1130–1139. https://doi.org/10.1108/JFC-09-2022-0225.

Ibrahim, S. 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime, and Justice* 47:44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002.

Iversen, T. N., L. Larsen, and P. E. Solem. 2009. A conceptual analysis of ageism. *Nordic Psychology* 61 (3): 4–22. https://doi.org/10.1027/1901-2276.61.3.4.

James, B. D., P. A. Boyle, and D. A. Bennett. 2014. Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect* 26 (2): 107–122. https://doi.org/10.1080/08946566.2013.821809.

Judges, R. A., S. N. Gallant, L. Yang, and K. Lee. 2017. The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology* 8: 588. https://doi.org/10.3389/fpsyg.2017.00588.

Karagiannopoulos, V., A. Kirby, S. O. M. Ms, and L. Sugiura. 2021. Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review* 43 : 105615. https://doi.org/10.1016/j.clsr.2021.105615.

Kasim, E. S., N. R. Awalludin, N. Zainal, A. Ismail, and N. H. Ahmad Shukri. 2023. The effect of financial literacy, financial behaviour and financial stress on awareness of investment scams among retirees. *Journal of Financial Crime*. https://doi.org/10.1108/JFC-04-2023-0080.

Kazdin, A. E., H. C. Kraemer, R. C. Kessler, D. J. Kupfer, and D. R. Offord. 1997. Contributions of risk-factor research to developmental psychopathology. *Clinical Psychology Review* 17 (375): 406. https://doi.org/10.1016/S0272-7358(97)00012-3.

Kircanski, K., N. Notthoff, M. DeLiema, G. R. Samanez-Larkin, D. Shadel, G. Mottola, L. L. Carstensen, and I. H. Gotlib. 2018. Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging* 33 (2): 325–337. https://doi.org/10.1037/pag0000228.

Köttl, H., V. Gallistl, R. Rohner, and L. Ayalon. 2021. "But at the age of 85? Forget it!": Internalized ageism, a barrier to technology use. *Journal of Aging Studies* 59 : 100971. https://doi.org/10.1016/j.jaging.2021.100971.

Lazarus, S. 2019. Just married: The synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal* 69 (231): 15–33. https://doi.org/10.1111/issj.12201.

Lazarus, S. 2021. Demonstrating the therapeutic values of poetry in doctoral research: Autoethnographic steps from the enchanted forest to a PhD by publication path. *Methodological Innovations* 14(2). https://doi.org/10.1177/20597991211022014.

Lazarus, S. 2024. Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the "Black Axe" confraternity. *Deviant Behavior* 46 (4): 456–480. https://doi.org/10.1080/01639625.2024.2352049.

Lazarus, S., M. Button, and R. Kapend. 2022. Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice* 61 (3): 381–398. https://doi.org/10.1111/hojo.12485.

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*. https://doi.org/10.1016/j.jeconc.2023.100013.

Lazarus, S., M. Hughes, M. Button, and K. H. Garba. 2025. Fraud as legitimate retribution for colonial injustice: Neutralization techniques in interviews with police and online romance fraud offenders. *Deviant Behavior* 1–22. https://doi.org/10.1080/01639625.2024.2446328.

Longo, M. 2015. *Fiction and social reality: Literature and narrative as sociological resources*. Surrey: Ashgate Publishing Limited.

Loyens, K., and R. Paraciani. 2021. Who is the ("Ideal") victim of labor exploitation? Two qualitative vignette studies on labor inspectors' discretion. *The Sociological Quarterly* 64 (1): 27–45. https://doi.org/10.1080/00380253.2021.1974321.

Mannheim, I., E. J. Wouters, H. Köttl, L. C. Van Boekel, R. Brankaert, and Y. Van Zaalen. 2022. Ageism in the discourse and practice of designing digital technology for older persons: A scoping review. *The Gerontologist*. https://doi.org/10.1093/geront/gnac144.

Marquart, J. W., and R. A. Thompson. 2024. Exploring relation fraud, murder, and the fraud triangle. *Journal of Economic Criminology*. https://doi.org/10.1016/j.jeconc.2024.100061.

McGuire, M. & Dowling, S. (2013). Cybercrime: A review of the evidence. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

National Council on Aging, NCA (2023). The top 5 financial scams targeting older adults, retrieved: https://ncoa.org/article/top-5-financial-scams-targeting-older-adults

Nicholson, J., & McGlasson, J. (2020). CyberGuardians: Improving community cyber resilience through embedded peer-to-peer support. In DIS 2020 companion—Companion publication of the 2020 ACM designing interactive systems conference, 117–121. https://doi.org/10.1145/3393914.3395871

Nicholson, J., L. Coventry, and P. Briggs. 2019. "If it is important it will be a headline": Cybersecurity information seeking in older adults. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3290605.3300579.

ONS. (2023). Crime in England and Wales: Year ending March 2023. Retrieved from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023#:~:text=9.-,Fraud,2020%20(3.7%20million%20offences)

Parsons, L. T., and L. Pinkerton. 2022. Poetry and prose as methodology: A synergy of knowing. *Methodological Innovations* 15 (2): 118–126. https://doi.org/10.1177/20597991221087150.

Phillips, C. 2017. From 'rogue traders' to organized crime groups: Doorstep fraud of older adults. *British Journal of Criminology* 57 (3): 608–626. https://doi.org/10.1093/bjc/azw011.

Piterová, I. 2020. Older adults vulnerability to fraud: Narrative review study. *Work and Organizational Psychology* 49:1.

Rebovich, D., and L. Corbo. 2022. The distillation of national crime data into a plan for elderly fraud prevention: A quantitative and qualitative analysis of US Postal Inspection Service cases of fraud against the elderly. In *The new technology of financial crime*, 126–149. Melbourne: Routledge.

Redmiles, E. M. (2019). "Should I worry?" A cross-cultural examination of account security incident response. In 2019 IEEE Symposium on Security and Privacy (SP) (pp. 920–934). IEEE. https://doi.org/10.1109/SP.2019.00059

Ren, P., G. Hou, M. Ma, Y. Zhang, and J. Wang. 2023. Enhanced putamen functional connectivity underlies altered risky decision-making in age-related cognitive decline. *Scientific Reports* 13: 6619. https://doi.org/10.1038/s41598-023-33634-w.

Ren, P., M. Ma, Y. Zhuang, Y. Zhang, and J. Wang. 2024. Dorsal and ventral fronto-amygdala networks underlie risky decision-making in age-related cognitive decline. *GeroScience* 46: 447–462. https://doi.org/10.1007/s11357-023-00922-2.

Roberts, L. D., D. Indermaur, and C. Spiranovic. 2013. Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law* 20 (3): 315–328. https://doi.org/10.1080/13218719.2012.672275.

Rosch, E. 1978. Principles of categorization. In *Cognition and categorization*, ed. Eleanor Rosch and Barbara B. Lloyd, 27–48. Hillsdale: Lawrence Erlbaum.

Shao, J., Q. Zhang, Y. Ren, X. Li, and T. Lin. 2019. Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect* 31 (3): 225–243. https://doi.org/10.1080/08946566.2019.1625842.

Sikra, J., K. V. Renaud, and D. R. Thomas. 2023. UK cybercrime, victims and reporting: A systematic review. *Commonwealth Cybercrime Journal* 1 (1): 28–59.

Soares, A. B., and S. Lazarus. 2024. Examining fifty cases of convicted online romance fraud offenders. *Criminal Justice Studies* 37 (4): 328–351. https://doi.org/10.1080/1478601X.2024.2429088.

Soares, A. B., S. Lazarus, and M. Button. 2025. Love, lies, and larceny: One hundred convicted case files of cybercriminals with eighty involving online romance fraud. *Deviant Behavior* 1–24. https://doi.org/10.1080/01639625.2025.2482824.

Teaster, P. B., K. A. Roberto, J. Savla, C. Du, Z. Du, E. Atkinson, E. C. Shealy, S. Beach, N. Charness, and P. A. Lichtenberg. 2023. Financial fraud of older adults during the early months of the COVID-19 pandemic. *The Gerontologist* 63 (6): 984–992. https://doi.org/10.1093/geront/gnac188.

Tornstam, L. 1997. Gerotranscendence: The contemplative dimension of aging. *Journal of Aging Studies* 11 (2): 143–154. https://doi.org/10.1016/S0890-4065(97)90018-9.

United Nations (2023). World social report 2023: Leaving no one behind in an ageing world, retrieved from: https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2023/01/WSR_2023_Chapter_Key_Messages.pdf (accessed 13/08/2023)

Wall, D. S. 2010. *Cybercrime: The transformation of crime in the information age*. Cambridge: Polity Press.

Wen, J., H. Yang, Q. Zhang, and J. Shao. 2022. Understanding the mechanisms underlying the effects of loneliness on vulnerability to fraud among older adults. *Journal of Elder Abuse & Neglect* 34 (1): 1–19. https://doi.org/10.1080/08946566.2021.2024105.

Xing, T., F. Sun, K. Wang, J. Zhao, M. Wu, and J. Wu. 2020. Vulnerability to fraud among Chinese older adults: Do personality traits and loneliness matter? *Journal of Elder Abuse & Neglect* 32 (1): 46–59. https://doi.org/10.1080/08946566.2020.1731042.

Yar, M., and K. F. Steinmetz. 2019. *Cybercrime and society*. London: SAGE Publications Limited.
Znaniecki, Florian. 1934. *The method of sociology*. New York: Rinehart.