



Extended editorial: preventing fraud and cybercrime in an ageing society

Mark Button¹ · Vasileios Karagiannopoulos¹ · Julak Lee² · Joon Bae Suh³ · Jeyong Jung⁴

Accepted: 12 April 2025
© The Author(s) 2025

Introduction

The nature of crime has been changing globally with technological and other societal developments fuelling a growth in fraud and cybercrime (Button and Cross 2017). The diversity and rapid evolution of a broad range of scams has led to millions across the globe becoming victims of fraud (Federal Trade Commission 2019; ONS 2023a, 2023b). A common belief often promoted in policy circles and some research is that older adults are more vulnerable to fraud (James et al. 2014). This is not so clear cut, however, as in terms of victimisation, the middle aged have been most at risk (see Fig. 1 later). This is changing and there is evidence older adults (65+) are fast becoming the one of the most at risk categories and that they also tend to lose much more than other age groups (see Table 1 later). Indeed, there are a variety of trends fuelling a potential explosion in fraud and cybercrime among older adults unless serious action is taken to reduce the risks that we will shortly explore. It is for this reason we conceived this special edition and the research project that underpins it.

To set the context for this edition, it is important to examine the factors fuelling the growth in fraud and cybercrime victimisation among older age groups. We will do this using data from the UK and South Korea. The reason for the selection of these countries is simple. The funding for the project stimulating this edition came from ESRC funding aimed at developing relationships with these two countries

✉ Mark Button
mark.button@port.ac.uk

✉ Julak Lee

¹ Centre for Cybercrime and Economic Crime, University of Portsmouth, Portsmouth, UK

² Chung Ang University, Seoul, South Korea

³ Korean National Police University, Asan, South Korea

⁴ University of Ulsan, Ulsan, South Korea



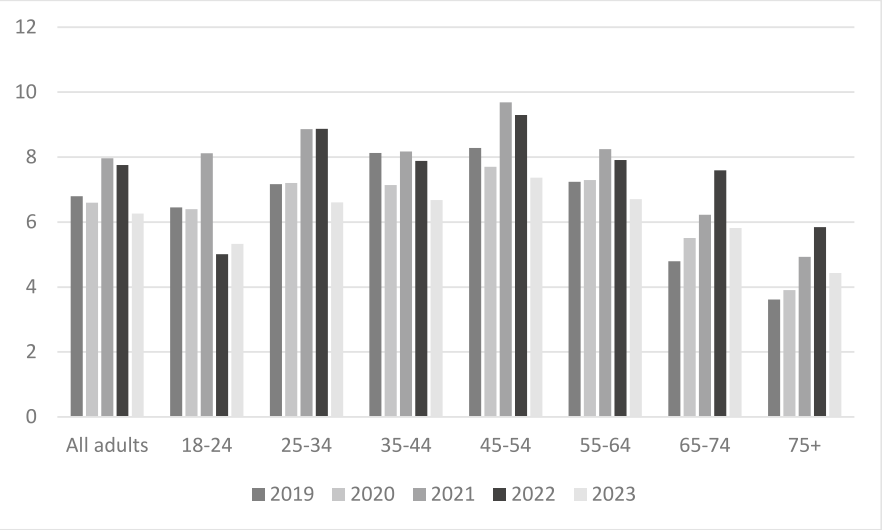


Fig. 1 Percentage of age groups victims of fraud in England and Wales. Note, from 2023 the 18–24 age group expanded to 16–24. ONS (2024)

Table 1 Average losses by age group reported to Action Fraud 2020–2022

Group 2020 2021 2022			
Age group	2020	2021	2022
18–24	£1251	£2922	£2052
25–34	£2189	£2554	£2970
35–44	£3724	£3995	£5135
45–54	£5868	£5605	£7135
55–64	£9229	£8445	£9392
65–74	£12,715	£9972	£10,231
75 +	£13,942	£13,428	£13,112

FOI request to action fraud

on issues such as ageing and technology. However, they are both highly developed countries with ageing populations experiencing a rise in fraud and cybercrime, so although the main reason is purely funding, they do provide two very useful case studies to illustrate the challenges and problems of ageing, fraud and cybercrime. The special edition, however, has papers from a much wider range of countries, including the USA, Australia, Brazil, UK, India and Nigeria too.

Older adults: fraud and cybercrime

Frauds and scams are often used interchangeably to describe deceptive behaviours that cause a person some form of financial loss. For instance, Button and Cross



(2017) note scams can be deceptive behaviours which cause a loss, which are clearly unethical, but lawful; whereas frauds are always unlawful. Another term important to grasp in this context is financial abuse, which is also a term with much debate on the scope, but generally considered to cover the improper or illegal exploitation or use of funds/resources of an older person (Fealy et al. 2012). It is also usually more associated with those close to the older adult such as family, carers or professionals working with them. Cybercrime is a much broader concept that covers both economic, psycho-social and state cybercrimes (Ibrahim 2016). This editorial and edition is only interested in economic cybercrimes: cyberfrauds, ransomware and hacking for monetary purposes, with a particular focus on: frauds, scams, financial abuse and economic cybercrime.

There are a number of methods of fraud and cybercrime which are common for older adults and types of fraud. Some of the more common include doorstep frauds/scams: rogue tradesmen who massively overcharge for their services and/or conduct works not required or to a poor standard. Door-to-door sales of non-existent or low quality services and/or goods (Phillips 2017). Financial abuse of older adults by carers, relatives or friends (Dalley et al. 2017). Telephone scams, where there is high pressure sales of worthless goods or service, particularly investments; impersonation scams that trick victims into transferring money and vishing, where sensitive personal information is sought (Choi et al. 2017; Lee 2020). Postal scams which utilise fake lotteries, bogus charities and investment schemes to name some touted through traditional mail (Rebovich & Corbo 2021). The Authorised Push Payment (APP) frauds where the victim is deceived into authorising a payment to a criminal via impersonation (National Fraud Authority 2011; Age UK 2023). Identity frauds: where victims are impersonated to use their financial credentials or identity fraudulently (Deliema et al. 2021; Cifas 2022). Finally, cyberfrauds: a wide range of scams using email, the internet and social media (Age UK 2017; Button and Cross 2017). The types of frauds and scams which particularly target older adults include:

- Consumer related frauds: sales of goods and services which are non-existent or worthless (Jorna 2016; Fan and Yu 2021).
- Investment related frauds: sales of bogus or overpriced investments (Deliema et al. 2020a, b).
- Romance and relationship frauds: bogus lovers and friends online who build up trust with aim to secure money from victim (Deliema 2018; Bailey et al. 2021).
- Impersonation of police/security frauds: fraudsters impersonate police and/or bank security staff with aim to trick victim into giving money or sensitive financial credentials away (Payne 2020; Benbow et al. 2022).
- Phishing-related frauds: a wide range of frauds seeking personal information related to victim (Choi et al. 2017; Button et al. 2021; Benbow et al. 2022).

In the previous years, COVID-19 also generated an additional layer of scams and financial abuse with safeguarding agencies reporting that community-dwelling adults had been targeted by pandemic-related scams regarding COVID-19 safety-related products. Risks for older adults have thus been exacerbated by the unavoidable increase in the use of technological tools for shopping, healthcare etc., which



has exposed this population to increased risks from cybercriminals, whilst making traditional risk assessments and safeguarding efforts more complex (Hakak et al. 2020; Benbow et al. 2022). Many older adults are lucrative potential targets, as large numbers have lifesavings, retirement ‘pots’ and investments.

In the past few years, COVID-19 has also exacerbated ageist discourses further enhancing perceptions of increased vulnerability of older adults and thus potentially highlighting them as ideal targets for criminals, particularly due to the increased isolation afforded by the pandemic, which distanced them even further from family and support networks (Han and Mosqueda 2020).

It is also clear from the literature that the impact of fraud on older adults can be devastating with not only the financial loss, but also psychological, physical and mental health and even suicide to name some (Button et al. 2014; Cross 2016b; Deliema et al. 2020a; Bailey et al. 2021; Button et al. 2021, 2024a, b). Research from Korea has also found that as the number of people aged 65 or older and the elderly living alone increases, frauds also tend to increase, and frauds also affect the suicide rate in the following year. The researchers collected crime and administrative data from all 215 regions in South Korea for five years from 2015 to 2019, built panel data and analysed them using fixed effect models. According to the study, frauds tend to increase as the population ages, and those over 65 or those living alone are more likely to be victims of fraud than other age groups. It seems that the ability to respond to scammers who use highly intelligent methods declines as the elderly population increases. Since the relationship between fraud victimization and suicide is highly likely to occur in the older adults, the researchers argued it is necessary to introduce fraud prevention education (Cho et al. 2021). Reports in the news in the UK in February 2023 also suggested fraud in England and Wales would be upgraded to a national security threat, such is the impact of it, with evidence that the crime puts 300 people a year in such a state of harm they are a suicide risk (Telegraph 2023).

Fraud trends

In recent years, older adults in England and Wales have become more likely to become victims of fraud. Figure 1 below illustrates the fraud victimisation rates across a range of age categories from 2019 to 2023. Victimization rates increased across all age categories during the pandemic but, excluding that period, have remained relatively stable with the exception of the 65–74 and 75+ age groups, where there has been a continuing upward trend.

Older adults may not be the most at risk group, but they tend to lose more. Table 1 below shows as the age rises so does the average losses, with the 65–74 and 75+ losing the most. Many of these are in positions in life where it is harder to recover from losses, due to fixed pensions.

The risk of being a victim of fraud is also increasing for older adults in South Korea. In 2018, there were about 267,000 fraud crimes nationally, which peaked at about 345,000 in 2020, and the most recent figure is about 325,000 in 2022. The overall number of fraud crimes has shown an upward trend, even though the number



of fraud crimes between 2019 and 2021 has fluctuated. On the other hand, the number of victims of fraud among those aged 60 and over is increasing more rapidly. In 2018, the number of cases of older adult victims increased from about 20,000 to about 46,000 in 2022, showing a steady upward trend. If we calculate the proportion of fraud crimes against older adults in the total number of fraud crimes, it is found that the proportion has more than doubled in four years, increasing from about 7.5% in 2018 to about 14.2% in 2022. This means that whilst the number of frauds against older adults is increasing not only in absolute numbers, it is also increasing as a percentage of all frauds.

Ageing in the UK and South Korea

Ageing in itself does not cause greater fraud, but there are additional factors associated with it that do. Before these are explored it is important to consider the significant ageing of the UK and Korean populations which is taking place. In the UK by mid-2020, there were 1.7 million people 85+ years—2.5% of the UK population. By mid-2045, this is projected to nearly double to 3.1 million, 4.3% of the total UK population (ONS 2022b). In South Korea, the proportion of the population aged 65 or older was 15.7% in 2020, will be 20.3% in 2025, and 25% by 2030 and it is expected that the current ageing society will enter a super-aged society (South Korea. Korean Statistical Information Service. 2023). Table 2 below illustrates the large numbers of older adults in the UK and South Korea across older adults age categories with in the UK around 15 million and in South Korea almost 12 million.

Macro factors fuelling fraud

Health of older adults

An ageing population brings with it some significant health challenges with larger numbers of older adults experiencing health conditions which may increase their

Table 2 Total number of older adults in the UK and South Korea

Age group	UK	South Korea
60–64	3,855,818	4,067,484
65–69	3,355,381	3,066,136
70–74	3,363,906	2,145,118
75–79	2,403,759	1,551,840
80–84	1,726,223	1,201,647
85–89	1,049,866	777,432
90 and older	609,503	
Total	16,364,456	12,809,657

ONS (2022a, b, c) and KOSIS (2023)
For UK data is 2021, for South Korea 2022



risk of becoming fraud victims. These include dementia, declining mental and physical health to name some. Declining cognitive ability has been linked in several studies to increased risk of fraud (James et al. 2014; Duke Han et al. 2015; Judges et al. 2017; Ueno et al. 2021). Severe dementia is not the largest risk of fraud because by this point the individual usually has a third party looking after their financial affairs (although this does open up a bigger risk of financial abuse). Mild and moderate dementia are seen as the greater risk to fraud victimisation as at this stage they are likely to control their financial affairs and their cognitive decline may make them less resilient to frauds and scams (Ueno et al. 2021). In the UK in 2019, the number of older adults with mild dementia was 126,900 and with moderate, 245,600. By 2040, this is set to increase by 55% for mild to 196,000 and by 33% for moderate to 327,500 (Wittenberg et al. 2019). In South Korea, the estimated number of people aged 65 and over with dementia as of 2020 was 840,000, with an estimated dementia prevalence rate of 10.3% (National Institute of Dementia 2023). This means that 10 out of every 100 people aged 65 and over are estimated to have dementia. The number of patients with mild cognitive impairment, a pre-dementia stage, also exceeded 150,000 and 357,506 with moderate dementia in 2020 (Ministry of Health and Welfare 2022). According to the National Institute of Dementia (2023), the estimated number of dementia patients in Korea is expected to reach 1.36 million in 2030 and exceed 3 million in 2050.

Burton et al. (2022) highlight one fifth of people aged 65+ experience some level of cognitive impairment, with many of those being Internet users opening up opportunities for a wide range of fraud victimisation. Mental illness is also a problem among older adults. In the UK, depression affects around 22% of men and 28% of women aged 65 years and over. It is estimated that 85% of older people with depression receive no help at all from the NHS. It is estimated 7–17% of older adults suffer from social isolation and this is set to continue to grow (Health and Social Care Information Centre 2007). As was noted earlier depression has been linked to greater risk of fraud victimisation (Lichtenberg et al. 2013; Burnes et al. 2017; DeLeima et al. 2020a, b).

Physical health is also an important factor because a decline can decrease mobility, increase social isolation and mean greater time spent at home. All of these factors are associated with increased risk of fraud (Ross et al. 2014; Burnes et al. 2017; Burton et al. 2022). High blood pressure among men has also been linked as a factor linked with increased fraud victimisation (Lamar et al. 2022).

In the UK, an estimated 4 million older adults in the UK (36% of people aged 65–74, and 47% of those aged 75+) have a limiting long-standing illness, equating to 40% of all people aged 65+ (Horsfield 2017). Those living with frailty are at greater risk of disability, care home admission, hospitalisation, and death (Wirral 2018). Approximately, 3% of the population aged 65+ in England live with severe frailty, 12% with moderate frailty and 35% with mild frailty (BMA 2018). As age rises, the proportion of people living with frailty increases: 6.5% in those 60–69; 65% in those 90+ (Gale et al. 2015). Mobility difficulties are also common among those living with frailty (93% have difficulties vs only 58% of non-frail individuals) (Gale et al. 2015). The ageing trends means this will increase rates of frailty further.



In South Korea, the situation is similar. Among older adults 37.0% thought, they were healthy, and 39.7% thought they were unhealthy (Lee 2018). More than half of older adults live with 3 or more chronic diseases, and the rate of 2 or more is 73.0%. About 3/4 of the elderly have overlapping chronic diseases (Lee 2018). Approximately, 89% of older adults in South Korea suffer from one or more chronic disease and considering Korea's life expectancy of 82.7 years and healthy life span of 64.4 years, older adults are predicted to live in an unhealthy state for about 10 years or more (South Korean Ministry of Health and Welfare 2017). In 2017, more than 40% of patients who received hospital treatment for depression were aged 60 or older. Among them, 30.2% of the elderly living alone, 16.4% of the elderly living with a spouse and 21.7% of the elderly living with adult children experienced depression (South Korean Ministry of Health and Welfare 2017; Won and Kim 2020).

Living alone and older adult households

Loneliness and/or living alone has also been linked with increased risk of fraud victimisation (Alves and Wilson 2008; Peterson et al. 2014; Cross 2016b; Xiang et al. 2020; Wen et al. 2022), along with the associated issues of lack of social networks, family, friends etc. (Deliema 2018; DeLeima et al. 2020a, b). England and Wales has a large number of households with those 66 and over living alone at 3.2 million (ONS 2022b). In South Korea, there is also a trend towards greater numbers of older adults living alone. The proportion of older adults living alone has increased from 16.0% in 2000 to 20.8% in 2022 amounting to 1,875,270 older adults (Statistics Korea 2022). Living alone and social isolation have also been linked with increased risk of fraud victimisation (Cross 2016a; Deliema 2018; DeLeima et al. 2020a, b).

Use of technology

There is much research linking routine activities theory to fraud victimisation (Holt and Bossler 2008; Reyns 2015; Leukfeldt & Yar 2016). Naturally the more time a person spends doing something the greater chance they will stumble across a situation that provides an opportunity for a fraudster to exploit. Thus more time spent shopping online increases the risk of shopping fraud, dating online leads to romance fraud, banking online lead to online banking fraud to name some. There are significant numbers of older adults who do not engage in these activities at present, but this looks set to change with increased opportunities for fraudsters to exploit with older adults with limited digital skills.

The use of the internet is a key vector towards fraud and cybercrime. Over the last decade there has been a substantial increase in the use of the internet among older adults in the UK. In 2013, 3.5 million of 65–74-year olds had used the internet in the past three months, had grown to 5.5 million in 2020 and for 75+ the increase had gone from 1.3 million to 2.9 million during the same period (ONS 2021). Perhaps even more significant is that for the numbers who had never used the internet; for 64–74 year olds fell from 1.9 million to 736,000 and for 75+ 3 million to 2.1 million



between 2013 and 2020. In South Korea for those aged in their 60 s, the internet usage rate increased by 12.0% to reach 94.5% and in the 70 s and older age group, it increased by 17.9%, approaching half (49.7%) of all households (National Information Society Agency, 2022).

The use of smartphones and related technologies has also increased among older adults. Just between 2018 and 2019, the percentage of older adults aged 65–74 increased from 40 to 43% and for 75+, 14% to 23%. In 2019, 25% of 65–74 year olds possessed a mobile phone with access to the internet and 13% of 75+. The possession of a tablet rose from 19 to 26% for 75+, but fell from 42 to 36% for 65–74 year olds. However, for both age groups there was a rise in the ownership of desktop computers, rising from 8 to 13% for 75+ and 19–23% for 65–74 year olds (OFCOM 2020). In South Korea, 83% of 60+ year olds use a smartphone (Gallup 2021). It seems that the use of smartphones among the elderly in South Korea is very high.

There is also evidence in the UK of a lack of skills among many older adults to use the internet and related technologies safely. Research has found limited knowledge of privacy and security threats—issues with digital literacy, with some more isolated and less able to engage in peer learning networks or assess quality advice (Tennant et al. 2015). The high fear of crime and perceived high susceptibility to threats can lead to disengagement with security measures and lower interaction with online services (Roberts et al. 2013; Nicholson et al. 2019). Older regular internet users are also not confident using the internet for finding security information or resolving security/technical situations—language challenges (Nicholson et al. 2019; Karagiannopoulos et al. 2021). There is also ignorance of reporting mechanisms—consequently low levels of reporting (Karagiannopoulos et al. 2021; Nicholson and Glasson 2020).

Wealth of older adults

Many older adults are also attractive targets as they have built up wealth during their working lives. In the UK between April 2018 and March 2020, the average wealth of someone 75+ was £271,800, 64–75 was £338,100, falling to £253,600 for the 45–64 age category, then to £52,000 for the 25–44 age category and only £15,100 for those in the 16–24 category (ONS 2022a, b, c). According to Korea's 2022 wealth statistics by age group, those aged 60 and over had KRW 483 million (£289,121), those aged 50–59 had KRW 534 million (£319,907), those aged 40–49 had KRW 469 million (£280,661), those aged 30–39 had KRW 299 million (£179,107) and those aged under 30 had KRW 84 million (£50,750) (Bank of Korea and Financial Supervisory Service 2022). Those in their 60 s and older owned fewer wealth than those in their 50 s, but more than any other age group.

Figure 2 above brings together the discussion above to illustrate the many factors associated which have been linked either directly to fraud or to factors associated with increased likelihood of victimisation. Some may be less important than others, but all are likely to have some impact on fraud victimisation and this illustrates the need for more research to truly appreciate the influences upon fraud victimisation among older adults and more generally. The section has also shown the strong push





Fig. 2 The fraud pressures for older adults

factors towards greater risks of fraud and cybercrime victimisation among older adults.

The future of fraud

Predicting the future is a notoriously difficult task, as Niels Bohr argued “Prediction is very difficult, especially if it’s about the future” (Cranfield 2013). There are however technological changes unfolding that when assessed in the context of previous fraud, one can make a reasonable assumption of potential new types of fraud. These will now be explored.

Fraud narratives

The most difficult to predict in the medium to longer term are the fraud narratives. Fraud narratives are constantly change and they tend to mirror more broader events and trends in wider society. So the energy price hikes following the Russian invasion of Ukraine triggered scams related to securing grants/refunds etc. related to energy bills. During the pandemic, there were a variety of scams that merged linked to it such as bogus protective equipment, government support grants etc. (Kemp et al. 2021). The narratives of frauds are constantly changing and it is difficult to predict



what these will be in the medium to longer term, but one can be attuned as a significant problem or event unfolds that fraudsters will be looking to exploit it. It is therefore futile trying to predict future fraud narratives above the immediate short-term. There are, however, other factors which we can be more confident of predicting as they relate to advances in technology which can be used to perpetrate frauds with the appropriate fraud narratives of the future.

AI-related fraud

AI has been written about extensively in relation to the potential to detect frauds. It has already and is likely to be increasingly used to perpetrate frauds against older adults and many other sections of the community.

(i) AI as selection tool

AI is likely to be used to select the most vulnerable victims. Scammers may use it to refine their selection criteria so they do not have to target as many victims and can be more confident that those they target will be more likely to become victims.

(ii) AI as content creator

AI through large language models like ChapGPT is already being used and likely to be used much more by fraudsters to write more persuasive scripts that are most likely to be successful with different types of victims (Europol 2023). Fraudsters with poor English will be able to develop much better quality text tailored to the victims and perhaps with more convincing arguments and related language. So, the old advice to look for poor grammar and spelling mistakes will be useless, whilst at the same time, the messaging will entail a higher degree of manipulative/social engineering potential. But more significantly fraudsters will be able to ask AI to write a persuasive request for a particular audience: women over 60, teenagers etc.

(iii) Realtime advisor

Linked to the above it will also be possible for fraudsters to develop real-time tools where scammers on the phone or chatting can use it to advice on most appropriate responses from victims. Again they will be able to tailor the responses by setting parameters to answer questions as if from a specific demographic.

(iv) AI an impersonator

AI is already been used in a wide range of scams to impersonate the voices and images of not just famous individuals but the loved ones of targets. This is likely to occur on a much larger scale. Scammers have already impersonated celebrities to orchestrate scams. In the UK, the leading consumer rights campaigner, Martin Lewis, was impersonated in a deep fake video which endorsed investments he did not (Money Saving Expert 2023). In China, scammers used deep fake technology to create videos to impersonate government officials asking potential victims to transfer monies to them. In India, scammers used such technology to change voices to



impersonate officials to target victims by telephone asking them to transfer monies (ACFE 2023).

Perhaps of even more concern will be the potential of AI to impersonate friends, family and work colleagues to trick them into giving money or information. Spear phishing targeting specific individuals has become a common scam, but AI will enable this to be taken to the next level as tools become freely available and widely used that enable fraudsters to impersonate the voices and eventually the images of associates of potential victims and then contact them to try and secure sensitive information or payments. Such frauds have already occurred when a Chief Executive's voice was cloned to trick his company into making a US\$220,000 payment (Wall Street Journal 2019). Researchers from Greece recently demonstrated the potential for deep fakes to trick virtual assistants to disclose personal information of their owners or engage in monetary transactions on their behalf, highlighting the need for enhanced security measures for VAs and more awareness on the side of users (Bilika et al. 2023).

The threat of these deep fakes will become more potent as AI is used to develop convincing voice messages for vishing, a threat particularly common for older adults and even video calls, which can make the scam even more convincing. The example of VALL-E voice cloning software is indicative of how deep fake voice messages can be developed with only seconds of a voice sample from someone and can then be used to breach bank accounts or get money from friends and family (Hauser 2023).

Metaverse

Another space where online fraud is expected to flourish in the coming years is the Metaverse and generally VR environments. Although the Metaverse transition seems to be slower than what Mark Zuckerberg expected, resulting in major losses for Meta, it seems that Meta environments, as currently heavily unregulated spaces could become fertile ground for old and new forms of fraud. According to Gartner Inc (2022): "By 2026, 25% of people will spend at least one hour a day in the metaverse for work, shopping, education, social and/or entertainment" whilst its economy will be dominated by cryptocurrencies and non-fungible tokens (largely unregulated), whilst many organisations are expected to gradually develop products and services for the Metaverse. In this environment, Smaili and De Rancourt-Raymond (2022) highlight that there can be a variety of considerations for cyberattacks, privacy breaches and identity theft. Mystakidis (2022) underlines the risk of tracing Metaverse avatars back to their offline users and the potential for social engineering through the collection of avatar-related information of victims by more experienced users. According to Kadar(2022), the largely unregulated nature of cryptocurrencies and NFTs, will also generate opportunities for associated scams and fraud, such as phishing for NFT account hacks.



Exploiting technological skills deficits

As more and more services move online and it becomes increasingly difficult to access services such as banking, customer service, online accounts etc. in-person or even on the telephone, there will be a minority of persons with limited skills who will struggle to access services, particularly the elderly or individual with disabilities (Karagiannopoulos et al. 2021). For example, a study found that older adults demonstrated anxieties linked with adopting new technologies and feelings of “inferiority and powerlessness” caused by a lack of technological expertise (Wu et al. 2015). The European Commission 2020 Eurobarometer report on Europeans’ attitudes towards cyber security (cybercrime) also highlighted that only 36% of those aged 55 and older feel well informed about the risks of cybercrime with just 14% of the same age group being aware of existing channels for reporting cybercrime. Consequently, we can expect that as we are transitioning to environments that require more in-depth awareness of technology and involve more advanced and perhaps even yet unknown victimisation risks, individuals lacking the capability or familiarisation with new technologies will be further disadvantaged at preventing and dealing with technology dependent or facilitated scams and other cyberattacks.

Introducing this edition

The discussion above has made clear the risk to older adults of fraud and cybercrime in the future from both a growing proportion of the population exhibiting traits that put them at more risk of victimisation, juxtaposed to a number of factors that will make the potential frauds that can be developed more potent.

This edition was framed from an ESRC funded research project directed at improving relations between the UK and South Korea on a research topic related to ageing and technology. The investigators, who are also the authors of this editorial embarked on a variety of research projects, some of which have already been published (see Button et al. 2024a, b, 2025a). As part of the project seminars and conferences were held, there was also an objective to develop a special edition of a journal dedicated to this subject. This edition is the result of that containing 12 papers from writers not just from the UK and Korea, but the USA, Australia, Brazil, China, Nigeria and India too.

The edition includes an impressive range of papers exploring the modus operandi and the factors of victimisation regarding fraud and cybercrime against older adults in countries where there is limited research on this issue such as India, Nigeria, Brazil, China and South Korea (Datti et al. 2025; Kim et al. 2025; Lazarus et al. 2025; Porto-Bellini 2025; Shapiro 2025; Uroko and Obiorah 2025), as well countries such as the USA and Australia where there is already much research (Cross and Holt 2025; Viana et al. 2025). The edition highlights the problem of fear of fraud for older adults, widely noted for many other crimes, but not for fraud (Button et al. 2025b). Very importantly the edition includes cutting edge papers illustrating theoretical and practical prevention-focussed analyses using both technology-based



solutions (Robinson and Edwards 2024; Qiu 2025), as well as more traditional policies (Lee et al. 2025; Parti 2025).

This editorial has noted fraud and cybercrime against older adults looks set to be a significant problem for the future. This edition's papers provide a strong foundation for the debates and research on this issue that will no doubt emerge in coming years. It is only a start and much more research is required, but we hope together it stimulates ideas and most of all you enjoy it!

Funding This project was made possible through funding from the Economic and Social Research Council (ESRC), Grant number ES/W011182/1.

Declarations

Competing interests The authors have no interests to declare.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- ACFE. 2023. AI: The Next Frontier for Fraudsters. <https://www.acfeinsights.com/acfe-insights/2023/6/23/ai-the-next-frontier-for-fraudsters#:~:text=Fraudsters%20are%20using%20AI%20to,law%20enforcement%20and%20regulatory%20bodies.&text=In%20May%202023%2C%20a%20group,officials%20and%20call%20unsuspecting%20citizens.>
- Activities Theory and Source-Path-Goal Metaphorical Study
- Age UK. 2017. Older People, Fraud and Scams. https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_oct17_scams_party_conference_paper_nocrops.pdf.
- Age UK. 2023. Age UK Successfully Campaigns for Older Victims of APP Scams. <https://www.ageuk.org.uk/discover/2023/january/successful-campaign-for-victims-of-app-scams/>.
- Alves, L. M., and S. R. Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of Elder Abuse & Neglect* 20 (1): 63–85.
- Bailey, J., L. Taylor, P. Kingston, and G. Watts. 2021. Older adults and “scams”: Evidence from the mass observation archive. *Journal of Adult Protection* 23 (1): 57–69. <https://doi.org/10.1108/JAP-07-2020-0030>.
- Benbow, S. M., S. Bhattacharyya, P. Kingston, and C. Peisah. 2022. Invisible and at-risk: Older adults during the COVID-19 pandemic. *Journal of Elder Abuse & Neglect* 34 (1): 70–76.
- Bilika, D., N. Michopoulou, E. Alepis, and C. Patsakis. 2023. Hello Me, Meet the Real Me: Audio Deepfake Attacks on Voice Assistants. <https://arxiv.org/pdf/2012.08347>.
- BMA. 2018. BMA—Identification and Management of Patients with Frailty. <https://www.bma.org.uk/advice/employment/contracts/general-practice/funding/focus-on-identification-and-management-of-patients-with-frailty>.
- Burnes, D., C. R. Henderson Jr., C. Sheppard, R. Zhao, K. Pillemer, and M. S. Lachs. 2017. Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health* 107 (8): e13–e21.



- Button, M., and C. Cross. 2017. *Cyber Frauds, Scams and Their Victims*. Taylor & Francis.
- Button, M., C. Lewis, and J. Tapley. 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27:36–54.
- Button, M., D. Blackburn, L. Sugiura, D. Shepherd, R. Kapend, and V. Wang. 2021. From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics* 64 : 101675.
- 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.
- Button, M., D. Shepherd, C. Hawkins, and J. Tapley. 2024b. Fear and phoning: Telephones, fraud, and older adults in the UK. *International Review of Victimology*. <https://doi.org/10.1177/02697580241254399>.
- Button, M., B. Hock, J. B. Suh, and C. S. Koh. 2025a. Policing cross-border fraud 'Above and below the surface': Mapping actions and developing a more effective global response. *Crime, Law and Social Change* 83 (1): 5.
- Button, M., D. Shepherd, C. Hawkins, and J. Tapley. 2025b. Fear of fraud among older adults: A hidden epidemic? *Security Journal*. 31:117.
- Burton, E., K. Hill, K. A. Ellis, A. M. Hill, M. Lowry, R. Moorin, J. A. McVeigh, A. Jacques, K. I. Erickson, J. Tate, and S. Bernard. 2022. Balance on the Brain: a randomised controlled trial evaluating the effect of a multimodal exercise programme on physical performance, falls, quality of life and cognition for people with mild cognitive impairment—study protocol. *BMJ open* 12(4):e054725.
- Cho, Y., J. Suh, H. Kim. 2021. The Analysis of Causes of Increasing Fraud in South Korea. Korean National Police Agency Research Paper.
- Choi, K., J. L. Lee, and Y. T. Chun. 2017. Voice phishing fraud and its modus operandi. *Security Journal* 30:454–466.
- Cifas. 2022. This is Fraudscape 2022. <https://www.fraudscape.co.uk/>.
- Cranfield. 2013. Forecasting—Prediction is Very Difficult, Especially If It's About the Future! <https://blogs.cranfield.ac.uk/cbp/forecasting-prediction-is-very-difficult-especially-if-its-about-the-future/>.
- Cross, C. 2016a. 'They're very lonely': Understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy* 5 (4): 60.
- Cross, C. 2016b. Using financial intelligence to target online fraud victimisation: Applying a tertiary prevention perspective. *Criminal Justice Studies* 29 (2): 125–142. <https://doi.org/10.1080/1478601X.2016.1170278>.
- Cross, C., and T. J. Holt. 2025. Does age matter? Examining seniors' experiences of romance fraud. *Security Journal*. 2025:1.
- Dalley, G., M. Gilhooly, K. Gilhooly, P. Harries, and M. Levi. 2017. Exploring financial abuse as a feature of family life: An analysis of court of protection cases. *Elder Law Journal* 7 (1): 28–37.
- Datti, R., N. Mishra, M. Sirisety, and A. Tewari. 2025. Risk perceptions and safe behaviours on the internet among older adults in India. *Security Journal* 2:12.
- DeLiema, M. 2018. Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist* 58 (4): 706–718.
- DeLiema, M., D. Burnes, and L. Langton. 2021. The financial and psychological impact of identity theft among older adults. *Innovation in Aging* 5 (4): igab043.
- DeLiema, M., M. Deevy, A. Lusardi, and O. S. Mitchell. 2020a. Financial fraud among older Americans: Evidence and implications. *Journals of Gerontology—Series B Psychological Sciences and Social Sciences* 75 (4): 861–868. <https://doi.org/10.1093/geronb/gby151>.
- DeLiema, M., D. Shadel, and K. Pak. 2020b. Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research* 46 (5): 904–914.
- Duke Han, S., P. A. Boyle, B. D. James, L. Yu, and D. A. Bennett. 2015. Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease* 49 (3): 845–851. <https://doi.org/10.3233/JAD-150442>.
- European Commission. 2020. Eurobarometer Survey Report: Europeans' Attitudes Towards Cyber Security (Cybercrime). <https://europa.eu/eurobarometer/surveys/detail/2249>.
- Europol. 2023. ChatGPT The impact of Large Language Models on Law Enforcement. <https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf>.
- Fan, J. X., and Z. Yu. 2021. Understanding aging and consumer fraud victimization in the Chinese context: A two-stage conceptual approach. *Journal of Elder Abuse & Neglect* 2021:1–18.



- Fealy, G., N. Donnelly, A. Bergin, M. P. Treacy, and A. Phelan. 2012. *Financial abuse of older people: A review*. Dublin: NCPOP, University College Dublin.
- Federal Trade Commission. 2019. Mass Market Consumer Fraud in the United States: A 2017 Update. <https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf>.
- Gale, C.R., C. Cooper, and A.A. Sayer. 2015. Prevalence of Frailty and Disability: Findings from the English Longitudinal Study of Ageing. <https://www.ifs.org.uk/publications/7910>.
- Gallup. 2021. 2012–2021 Study of Smartphone Usage & Brands, Smartwatches, and Wireless Earphones (Gallup Report, 20210608). <https://www.gallup.co.kr/gallupdb/reportContent.asp?seqNo=1217>.
- Gartner Inc. 2022. Press Release: Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026. www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026.
- Hakak, S., W. Z. Khan, M. Imran, K. R. Choo, and M. Shoaib. 2020. Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. *IEEE Access* 8:124134–124144. <https://doi.org/10.1109/ACCESS.2020.3006172>.
- Han, S. D., and L. Mosqueda. 2020. Elder abuse in the COVID-19 era. *Journal of the American Geriatric Society* 68 (7): 1386–1387. <https://doi.org/10.1111/jgs.16496>.
- Hauser, K. 2023. New Voice Cloning AI Lets “You” Speak Multiple Languages. *Freethink*. <https://www.freethink.com/robots-ai/voice-cloning#:~:text=Given%20a%20sample%20of%20a,than%20the%20one%20originally%20spoken>.
- Health and Social Care Information Centre. 2007. Health Survey for England, 2005: Health of Older People. <http://www.hscic.gov.uk/pubs/hse05olderpeople>. Accessed 14 Sep 2015.
- Holt, T. J., and A. M. Bossler. 2008. Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior* 30 (1): 1–25.
- Horsfield, J. 2017. Later Life in the United Kingdom—Too Old to Care?
- Ibrahim, S. 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice* 47:44–57.
- 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 and Neglect* 26 (2): 107–122. <https://doi.org/10.1080/08946566.2013.821809>.
- Jorna, P. 2016. The relationship between age and consumer fraud victimisation. *Trends and Issues in Crime and Criminal Justice* 519:1–16.
- 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.
- Kadar, T. 2022. The Metaverse Fraud Questions: What are the Risks? SEON. <https://seon.io/resources/metaverse-fraud/>.
- 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.
- Kemp, S., D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño. 2021. Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice* 37 (4): 480–501.
- Kim, M., S. Hong, and J. Jung. 2025. The shadow of digital society: Why the elderly are vulnerable to online phishing—a case study from South Korea. *Security Journal*. 3:1.
- Lamar, M., L. Yu, S. Leurgans, N. T. Aggarwal, R. S. Wilson, S. D. Han, and P. Boyle. 2022. Self-reported fraud victimization and objectively measured blood pressure: Sex differences in post-fraud cardiovascular health. *Journal of the American Geriatrics Society* 70 (11): 3185–3194.
- Lazarus, S., P. Tickner, and M. McGuire. 2025. Cybercrime against senior citizens: Exploring ageism, ideal victimhood, and the pivotal role of socioeconomics. *Security Journal*. 2025:0955–1662.
- Lee, Y. 2018. Health and care of older adults in Korea. *Health and Welfare Forum* 10:19–30.
- Lee, C. S. 2020. A crime script analysis of transnational identity fraud: Migrant offenders’ use of technology in South Korea. *Crime, Law and Social Change* 74 (2): 201–218.
- Lee, Y., C. Koh, and J. Suh. 2025. Preventive counselling against online fraud: Does this work? *Security Journal*. 81:100744.
- Leukfeldt, E. R., and M. Yar. 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37 (3): 263–280.



- Lichtenberg, P. A., L. Stickney, and D. Paulson. 2013. Is psychological vulnerability related to the experience of fraud in older adults? *Clinical Gerontologist* 36 (2): 132–146. <https://doi.org/10.1080/07317115.2012.749323>.
- Money Saving Expert. 2023. WARNING: Beware Frightening New ‘deepfake’ Martin Lewis Video Scam Promoting a Fake ‘Elon Musk investment’—It’s Not Real. <https://www.moneysavingexpert.com/news/2023/07/beware-terrifying-new--deepfake--martin-lewis-video-scam-promoti/#:~:text=It%20is%20completely%20fake%20%E2%80%93%20Martin,of%20Martin%20uses%20his%20voice.>
- Mystakidis, S. 2022. Metaverse. *Encyclopedia* 2:486–497. <https://doi.org/10.3390/encyclopedia2010031>.
- National Fraud Authority. 2011. A Quantitative Segmentation of the UK Population Helping to Determine How, Why and When Citizens Become Victims of Fraud. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118481/national-fraud-segmentation.pdf.
- Nicholson, J., and J. McGlasson. 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’s 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>.
- OFCOM. 2020. Consumer Concerns: Experience of Nuisance Calls. <https://www.data.gov.uk/dataset/16dfac72-414e-4be9-98b7-585eabf7480d/consumer-concerns-experience-of-nuisance-calls>.
- ONS. 2021. Internet Users. <https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/datasets/internetusers>.
- ONS. 2022a. Estimates of the Population for the UK, England, Wales, Scotland and Northern Ireland. <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/datasets/populationestimatesforukenglandandwalesScotlandandnorthernireland>.
- ONS. 2022b. Demography and Migration Data, England and Wales: Census 2021. <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/demographyandmigrationdatacontent/2022-11-02#demography-household-characteristics>.
- ONS. 2022c. Individual Wealth: Wealth in Great Britain. <https://www.ons.gov.uk/peoplepopulationandcommunity/personalandhouseholdfinances/incomeandwealth/datasets/individualwealthingreatbritain>.
- ONS. 2023a. National Population Projections: 2020-Based Interim. <https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationprojections/bulletins/nationalpopulationprojections/2020basedinterim>.
- ONS. 2023b. Crime in England and Wales: Appendix Tables. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables>.
- ONS. 2024. Nature of Fraud and Computer Misuse in England and Wales: Appendix Tables. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables>.
- Parti, K. 2025. The wisdom of the scammed: Redefining older fraud victim support by utilizing the ecological systems framework. *Security Journal*. 2025:1.
- Payne, B. K. 2020. Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice* 45:563–577.
- Peterson, J. C., D. P. Burnes, P. L. Caccamise, A. Mason, C. R. Henderson, M. T. Wells, and M. S. Lachs. 2014. Financial exploitation of older adults: A population-based prevalence study. *Journal of General Internal Medicine* 29 (12): 1615–1623.
- Phillips, C. 2017. From ‘rogue traders’ to organized crime groups: Doorstep fraud of older adults. *British Journal of Criminology* 57 (3): 608–625. <https://doi.org/10.1093/bjc/azw011>.
- Porto-Bellini, C. 2025. Social engineering and vulnerability of user generations of digital technology: A routine activity theory and source-path-goal metaphorical study. *Security Journal*.
- Qiu, X. 2025. Policing AI-generated crimes: An ethnographic study on anti-cybercrime police in China. *Security Journal* 2025:1.
- Rebovich, D., and L. Corbo. 2021. The distillation of national crime data into A plan for elderly fraud prevention: A quantitative and qualitative analysis of U.S. postal inspection service cases of fraud against the elderly. *Victims and Offenders* 16 (3): 407–430. <https://doi.org/10.1080/15564886.2020.1865225>.



- Reyns, B. W. 2015. A routine activity perspective on online victimisation: Results from the Canadian general social survey. *Journal of Financial Crime* 22 (4): 396–411.
- Roberts, L. D., D. Indermaur, and C. Spiranic. 2013. Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law* 20 (3): 315–328.
- Robinson, J., and M. Edwards. 2024. Fraudsters target the elderly: Behavioural evidence from randomised controlled scam-baiting experiments. *Security Journal* 37:1–24.
- Ross, M., I. Grossmann, and E. Schryer. 2014. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science* 9 (4): 427–442. <https://doi.org/10.1177/1745691614535935>.
- Shapiro, L. 2025. Cyber-enabled imposter scams against older adults in the United States. *Security Journal*. 2025:3.
- Smaili, N., and A. de Rancourt-Raymond. 2022. Metaverse: welcome to the new fraud marketplace. *Journal of Financial Crime*. <https://doi.org/10.1108/JFC-06-2022-0124>.
- South Korea. Bank of Korea & Financial Supervisory Service. 2022. Household Financial Well-Being Survey 2022. <https://www.index.go.kr/unity/potal/indicator/IndexInfo.do?clasCd=10&idxCd=F0139>.
- South Korea. Korean Statistical Information Service (KOSIS). 2023. Census 2022 (Older Adults by Sex, Household Type, and Age—Municipalities). https://kosis.kr/statHtml/statHtml.do?orgId=101&tblId=DT_11N2010&conn_path=12.
- South Korea. Ministry of Health and Welfare. 2017. 2017 Results of Survey on the Condition of the Elderly. https://www.mohw.go.kr/react/jb/sjb030301vw.jsp?PAR_MENU_ID=03&MENU_ID=032901&CONT_SEQ=344953&page=1.
- South Korea. Ministry of Health and Welfare. 2022. Dementia Status by City and District 2020. <https://www.data.go.kr/data/15073342/fileData.do>.
- South Korea. National Information Society Agency. 2022. 2021 Survey on the Internet Usage. https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=99870&bcIdx=24378&deptCode=%27&parentSeq=24378.
- South Korea. National Institute of Dementia. 2023. Annual Report 2022. https://www.nid.or.kr/download/download.aspx?ver=PC&path=%2Fpapers%2F20230628143508306.pdf&filename=20230628143508306.pdf&ori_filename=%EC%A4%91%EC%95%99%EC%B9%98%EB%A7%A4%EC%84%BC%ED%84%B0_2022%EC%97%B0%EC%B0%A8%EB%B3%B4%EA%B3%A0%EC%84%9C.pdf.
- South Korea. Statistics Korea. 2022. Household Projections 2020. <https://www.index.go.kr/unify/idx-info.do?idxCd=8039>.
- Telegraph. 2023. Fraud set to be upgraded as a threat to national security. <https://www.telegraph.co.uk/news/2023/02/04/fraud-set-upgraded-threat-national-security/>.
- Tennant, B., M. Stollefson, V. Dodd, B. Chaney, D. Chaney, S. Paige, and J. Alber. 2015. eHealth literacy and Web 2.0 health information seeking behaviors among baby boomers and older adults. *Journal of Medical Internet Research* 17 (3): e70.
- Ueno, D., Y. Daiku, Y. Eguchi, M. Iwata, S. Amano, N. Ayani, and J. Narumoto. 2021. Mild cognitive decline is a risk factor for scam vulnerability in older adults. *Frontiers in Psychiatry* 2021:2365.
- Uroko, F., and M. Obiorah. 2025. Fraud and cybercrime against older adults in Christian-dominated southern Nigeria. *Security Journal*. 2:2.
- Viana, J., C. Porto-Bellini, A. Oguz, and R. de Faria Pereira. 2025. Social engineering and vulnerability of technology user generations: A routine. *Security Journal*. 141:156.
- Wall Street Journal. 2019. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. <https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>.
- 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* 34:1–19.
- Wirral, F. 2018. Frailty. https://www.wirralintelligenceservice.org/media/2510/frailty_review_final_7-8-2018.pdf.
- Wittenberg, R., B. Hu, L. Barraza-Araiza, and A. Rehill. 2019. *Projections of Older People with Dementia and Costs of Dementia Care in the United Kingdom, 2019–2040*. London: London School of Economics.
- Won, S., and H. Kim. 2020. Social participation, health-related behavior, and depression of older adults living alone in Korea. *Asian Social Work and Policy Review* 14 (1): 61–71.



- Wu, Y. H., S. Damnée, H. Kerhervé, C. Ware, and A. S. Rigaud. 2015. Bridging the digital divide in older adults: A study from an initiative to inform older adults about new technologies. *Clinical Interventions in Aging*. <https://doi.org/10.2147/CIA.S72399>.
- Xiang, H., J. Zhou, and B. Xie. 2020. Understanding Older Adults' Vulnerability and Reactions to Telecommunication Fraud: The Effects of Personality and Cognition. In *International Conference on Human-Computer Interaction*, ed. Q. Gao and J. Zhou, 351–363. Cham: Springer.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

