DAWES CENTRE FOR FUTURE CRIME AT UCL

Older adults as victims of online financial crime

Summary

Older people* are the fastest growing demographic of internet users. This brings multiple benefits including access to services and social connectivity, but also new risks of becoming a victim of online financial crimes, including credit card fraud and identity theft. While people of all ages are susceptible to becoming victims of such crimes, there are a number of risk factors affecting older people in particular, such as a lower familiarity with technology and social isolation.[1,2]
This briefing summarises research that explored how and why older adults become victims of online financial crime and investigates possible ways to address it, based on the findings of a literature review and cross-sector workshop.[3]

Introduction

For all age groups, living online offers new opportunities to become a victim of crime. Cybercrime can be defined as “any criminal activity in which a computer (or networked device) is targeted or used”. Financial cybercrime includes consumer frauds and scams designed to obtain financial benefit by deceiving a victim, including phishing (scam) emails or text messages which direct users to harmful websites that download viruses, or steal passwords, bank details or other sensitive information.

The use of the internet is growing rapidly amongst older age groups.* The proportion of over 55s who said they’d recently used the internet rose from 67% in 2015 (compared to 97% of 16-54s) to 81% in 2020 (compared to 99% of 16-54s).[4] The Covid-19 pandemic further encouraged new digital users from older age groups, offering benefits for accessing services and social media. However, this could also increase their risk of becoming a victim.[5] Fraudsters are opportunistic, for example purporting be from HMRC offering a tax refund owing to Covid-19, but directing victims to a fake website to harvest their personal and financial details.[6]

While official statistics do not indicate that older people are at increased risk of online financial crime, among certain groups of older people there is an increased risk due to a combination of factors such as low familiarity with technology, isolation or cognitive impairment. It is important to specifically consider older people as victims of online financial crime, so more older people are able to safely access and benefit from the internet.

Key facts

5 hours

Average time over 65s spent online per day during the first lockdown

65%

Proportion of over 65s who report using social media

26%

Proportion of over 65s using the internet who reported experience of an online fraud attempt during the first lockdown.

These findings are based on a Dawes Centre for Future Crime/ Neighbourhood watch survey. From sample of 7903 over 65s between 23 March-4 July 2020.

UK Policy context

Following the 2019 Online Harms White Paper and public consultation, the Draft Online Safety Bill was published in May 2021. Regulated by Ofcom,[7] the Bill will introduce a duty of care for companies to take greater responsibility for the safety of their users and to tackle the harms caused by content or activity on their services.[8] The Bill initially excluded all online fraud which was deemed to be out of scope. After pressure from regulators and the financial sector, in late 2020 user-generated online scams – including romance scams and fake investment opportunities, were included in the draft Bill.

Online fraud and scams via advertising, emails or cloned websites still fall outside the scope of the draft Bill, although they could be captured by the broader obligations on platforms to protect against illegal content.[7] The Home Office are also developing a new Fraud Action Plan for 2022-2025, which is now due to be published.

This research is relevant to the current UK policy agenda which seeks to address online financial crimes. While fraud is covered as a criminal offence under the Fraud Act 2006, this has not stopped the crime taking place and unfortunately many crimes are not reported, and many of those that are do not result in prosecution.[9,10]

The findings of the research summarised in this briefing highlights the challenges of considering victims as one group and the need to more closely investigate unique risk factors of certain demographics, including older people.

Methods

- A **realist review** (a type of literature review) investigated how, why and in what circumstances older adults become victims of financial cybercrime. The authors reviewed 53 academic papers, policy reports and other publications.
- A **sandpit event** (workshop) was held online in November 2020 with 21 representatives from Government, law enforcement, academia, the third and financial sectors. Participants reviewed the data collected, considered how it related to their experiences, and were asked to identify scenarios where the risk of victimisation was high for older people.

How are older adults at risk of becoming victims of financial cybercrime?

The review identified risk factors for older people becoming victims of online financial crime, which can be grouped into three overarching themes: cybersecurity skills and behaviours, social and health-related issues, and societal context.

Ranking exercise

Workshop participants were asked to rank the most harmful and profitable types of online financial crime. The top three in terms of their potential to harm and for profitability to the offender were:

Romance scams: An older person is befriended on a social networking or dating site. Once the scammer has gained the victim's trust, they ask for money, supposedly to help get them out of a difficult situation. It is a form of extortion using "emotional blackmail".

2. Identity theft: An older person's personal data is wrongfully obtained and used in some way that involves fraud or deception, typically for economic gain (such as to get a bank loan).

3. Cyberfraud by family members: Use of the internet by family members to trick an older person out of money, property or inheritance.

Cyber security skills and behaviours

Limited skills/awareness of security threats

People with limited skills and awareness of cyber security threats may be less motivated and/or aware of how to protect themselves and more likely to share personal details (such as on social networking sites). They may also have less familiarity with online security language, be less likely to seek out cyber security information or less able to identify illegitimate online content or emails.

While many older adults, especially those who have used computers at work are highly proficient in managing their online affairs, as a group they tend to have had fewer years of exposure to technology, and thus less awareness and cyber security skills.[11]

Receiving poor quality advice

Evidence shows that older adults are more likely to seek out quick and simple solutions to accessing online services. For example, approaching someone with limited expertise because they are local or easily contactable – perhaps a friend or neighbour.[2] They are also less likely to adopt PIN or biometric protections – such as setting a password, installing antivirus software or creating back-up files, motivated by a preference for ease of accessing services over security.

Vulnerability to certain types of scam

Older adults are more likely to respond to communications from legitimate-looking sources, such as a bank, the police or a government department. Previous research has suggested this relates to a greater generational trust in authority. For example, a message may allege that there are issues with a payment, account security or that a refund is due, with the aim of gaining valuable account details that should be kept private.

Social and health-related issues

Declining health and mobility

Older adults are more likely to experience declining health and mobility. This can result in an increased reliance on online banking, health care and social media services. This consequent need to share personal details more frequently increases the risk of identity theft.

Memory problems and cognitive deficits

Short-term memory problems are more common with advancing age, as the likelihood of experiencing dementia or Mild Cognitive Impairment (MCI) increases. Memory problems may reduce awareness or understanding that a crime has taken place, and make it difficult to recall details of the crime or offender, and thus to report a crime.

Cognitive deficits (including judgement or impulsivity) and/or reduced perceptual speed (slower processing of sights and sounds) also affect older people with MCI or dementia. This may leave people less able to understand and evaluate choices.

For example, research has found that people with MCI were less able to recognise scams such as email phishing. Other issues affecting people with cognitive deficits include being less likely to follow recommended password guidelines or to consider the repercussions of sharing personal information.

Social isolation and loneliness

Older people are more likely to have smaller social networks and live alone. This reduces opportunities to discuss potential scams and seek advice from others when they have concerns or doubts about the legitimacy of online requests.

There are 1.4m chronically lonely older people in England.[12] Loneliness can provide an initial motivation for an older person to try to meet people online, increasing their online visibility to potential offenders. It also provides the means through which offenders can establish a relationship with them. Fraudsters can create a sense of trust that increases the victim's willingness to act on their guidance or advice. As with other types of fraud, 'grooming' or befriending is common in investment fraud, and these can often result in significant financial losses.

Bereavement

Taking on financial responsibilities at a time of stress and grief after bereavement may impact an older person's ability to identify scams and leave them more at risk of becoming a victim. This is particularly true in cases where the deceased partner had previously been responsible for the couple's financial matters.

Wealth

Many older people have varied financial assets (such as property, savings and good credit scores), making them good targets for fraudsters. They are also less likely to check their balance online between printed statements, making them less likely to identify and report financial losses and more likely to be subject to repeated offences.

Societal context

Stereotypes about victims

There is a sense that financial cybercrime is not perceived as serious by society and negative stereotypes can portray victims as greedy or gullible. This may create feelings of embarrassment, shame or a fear of not being taken seriously amongst victims. For many victims, including older people, this victim-blaming culture can exacerbate the impact of crime and act as a barrier to accessing support or reporting victimization.

Perceptions of vulnerability

Older people may fear that disclosing financial cybercrime will be interpreted as a decline in their capacity or ability to care for themselves or their financial affairs, and that they may lose their independence as a result.

Ideas for interventions

There is limited evidence of evaluated interventions aimed at protecting older adults from becoming victims of cybercrime. Sandpit participants suggested ideas for interventions, grouped here by the same three overarching themes used above, with an additional final suggestion:

Cyber security skills and behaviours

- Increasing knowledge, awareness and peer support for older people without cognitive impairments. For example, using a solutions-based approach ("this is how you resolve the issue” rather than “you are at risk”) training sessions, with peer-learning involving social interactions.

Social and health related issues

- Information campaigns targeting workers and family members who support older online users could usefully include strategies for detecting and managing incidents of cybercrime, including situations where victims are unaware of frauds.
- Training on cybercrime detection and prevention for health and social care, third sector and other public workers such as librarians, who have frequent contact with older people was suggested as an intervention for safeguarding people with cognitive impairments.
- Artificial intelligence approaches to enhance the usability of security software for people with cognitive impairments. For example, tools to simplify and promote the use of biometrics that do not require password recall (such as facial recognition), or provide warnings to people when their online visibility is high (such as a public social media profile).

Societal context

- Provision of education and communication skills training for those supporting victims of online fraud (police, charity workers, health, and social workers) and positive campaigns from financial institutions to raise awareness and address societal perceptions about cybercrime victims, focused on empathy rather than blaming victims.
- Raising awareness among providers of financial services and online platforms about the particular risks faced by older people, to enable the design of more secure systems.

A different suggestion was that interventions could target the behaviours of offenders rather than victims. Behavioural management programmes aimed at reducing repeat offending could be a way to promote offenders to reflect on the impacts of the crime on their victims. Cybercrime offenders don’t usually meet their victims to see the impact of their crimes, and perhaps using victim’s stories could try to bring this to the fore.

References

1. Nicholson J, Coventry L, Briggs P. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems; Glasgow, Scotland, UK2019. p. 1-11.

2. Age UK, 2015. Only the tip of the iceberg: Fraud against older people. Evidence Review. Available at: https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-homerb_april15_only_the_tip_of_the_iceberg.pdf

3. A pre-print of this research paper is available at: https://osf.io/preprints/socarxiv/qvdy3/ .

4.ONS, 2021. Dataset on Internet Users. Available at:https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/datasets/internetusers

5.Cybercrime against older people during COVID19 pandemic. https://www.ucl.ac.uk/jill-dando-institute/sites/jill-dando-institute/files/cybercrime_0.pdf

6. Crowe. The financial cost of fraud 2021. Available at: https://www.crowe.com/uk/insights/financial-cost-fraud-data-2021

7. UK Government, draft Online Safety Bill. https://www.gov.uk/government/publications/draft-online-safety-bill

8.House of Commons Library briefing, Online Safety Bill https://commonslibrary.parliament.uk/research-briefings/cbp-9214/

9.Bidgoli, M. & Grossklags, J., 2016. End user cybercrime reporting: what we know and what we can do to improve it. In *2016 IEEE ICCCF* (p. 1-6).

10. Action Fraud Cybercrime trends 2020-21. Available at: https:/www.actionfraud.police.uk/data

11.Blackwood-Brown C, Levy Y, D’Arcy J. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. Journal of Computer Information Systems. 2019;61(3):195-206.

12. Age UK, 2018. All the Lonely People: Loneliness in Later Life. Available at: https://www.ageuk.org.uk/our-impact/policy-research/loneliness-research-and-resources/

*NHS guidance states that someone over the age of 65 might be considered an older person. However, it is not easy to apply a strict definition because people can biologically age at different rates.

Our research

This work was carried out by the Dawes Centre for Future Crime at UCL. This briefing was produced in partnership with Florence Greatrix at UCL STEaPP’s Policy Impact Unit. The research was funded by the Dawes Centre for Future Crime at UCL.

Lead researchers

Dr Kartikeya Tripathi k.tripathi@ucl.ac.uk
Professor Claudia Cooper claudia.cooper@ucl.ac.uk
Dr Alexandra Burton a.burton@ucl.ac.uk

Contact us

https://www.ucl.ac.uk/jill-dando-institute/research/dawes-centre-future-crime
https://www.ucl.ac.uk/steapp/collaborate/policy-impact-unit-1