UCL JDI Special Series on COVID-19: No. 4
ISSN 2635-1625

UCL Jill Dando Institute of Security and Crime Science

Cybercrime against older people during COVID19 pandemic

Dr Kartikeya Tripathi, UCL JDI
Prof Claudia Cooper, UCL Psychiatry
April 2020

The problem

The COVID lockdown has increased the risks for older people of being a victim of cybercrime. Vulnerability factors for cybercrime--loneliness, anxiety, stress--are increased.

At the same time, increasing numbers of opportunist criminals are targeting vulnerable individuals online.

Research shows that specialised gangs target older people online, as they are especially vulnerable to frauds. In the lockdown, older people, like their younger counterparts, are spending more time online creating greater opportunities for exploitation.

What we know about cybercrime against older people and how we know it

As global internet penetration has increased, so have incidents of cybercrime. The proportion of populations across the world who are older (aged 60 years or above) is growing. Older people are also the fastest growing demographic group of novice internet users, commonly using the internet to access banking, shopping and healthcare management services and for social media and other communication. Like the rest of the population, the growing adaption of internet technology has exposed older adults to threats of online crime. Historically, older people have been a prime target for fraud because of factors including their relative wealth, loneliness, memory loss, being from a generation characterised by high levels of trust and hesitancy to report crime to authorities.

The online interfaces that older people use to conduct commercial transactions have a generic design and it is possible that these designs do not support older people to negotiate them securely. For example, memory loss has implications for use of passwords and memorable information, and older people may face challenges complying with the technical specifications on secure behaviour.

From the criminal's perspective, cybercrime against older people is a low risk crime. Victimisation is under-reported to the police and even among those crimes that are reported, very few end in arrests and convictions.

What we think might happen in the covid-19 pandemic

Extrapolating from the results of our cross-national inter-disciplinary study on cybercrime against older people, in collaboration with colleagues from UCL Psychiatry, we think that the COVID pandemic and societal response to it has created a perfect storm that criminals will exploit to victimise older people online. For example, older people are especially vulnerable to frauds that offer friendship/romance as a way out of loneliness, and for 'magic remedies' against health ailments they are worried about. It is likely that both these crimes will increase.

The lockdown also means that older people are more isolated. If they do not live with their family members, they may be less protected by family support when negotiating the online space.

The restrictions on movement imposed in response to Coronavirus have pushed older people to bank and shop online. In cyberspace, there are no special safeguards or support available for older people as it is in

physical shops and bank branches. Moreover, unfamiliarity with technology and possibly a greater level of trust in earlier generations can make older people easy targets for motivated offenders. Social engineering frauds, credit card and romance scams are some of the crime categories that will surge as a result of conditions created by the pandemic.

Some ideas in response

Older people need to be recognised as a potentially vulnerable group that requires specific safeguards to protect them from cybercrime.

- Banks and online retailers should include special security features in their websites to protect older people
- Older people should get alerts on their phones via SMS whenever their bank accounts are used for a financial transaction
- Older people should have the option to reverse or stop payments immediately when they have been victims of an online fraud
- Banks and online retailers should increase awareness on their websites about fraudulent schemes against older people
- Special tools should be developed to teach secure online behaviour to older people
- The process of reporting online victimisation should be made simple, and older people encouraged to report all crimes
- GPs, council workers, pharmacists, post office and bank employees should be trained to identify signs of financial abuse in older people
- A database of websites, online handles and social media accounts that are involved in cybercrime against older people should be developed to keep track of offenders

Relevant resources

Age UK guide to staying safe online: https://www.ageuk.org.uk/information-advice/work-learning/technology-internet/internet-security/

Cook, D. M., Szewczyk, P., & Sansurooah, K. (2011). Securing the Elderly: A Developmental Approach to Hypermedia Based Online Information Security for Senior Novice Computer Users.

Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number…': Exploring seniors' attitudes towards identity crime. *Security Journal*, *30*(1), 74-88.

Vroman, K. G., Arthanat, S., & Lysack, C. (2015). "Who over 65 is online?" Older adults' dispositions toward information communication technology. *Computers in Human Behavior*, *43*, 156-166.

This is one of a series of short, speculative papers developed by the UCL Jill Dando Institute during the current pandemic. It is edited by Nick Tilley and Gloria Laycock and published by University College London. The raison d'être of the series is fully described at: https://www.ucl.ac.uk/jill-dando-institute/research/covid-19-special-papers