A brief report on older people's experience of cybercrime victimisation in Mumbai, India

Abstract

As internet penetration increases in Lower and Middle Income Countries (LMIC), more older people are now conducting financial transactions online and using social media to stay in touch with family and friends. We discuss concerns that existing financial regulations and controls in India may afford older people insufficient protection from cybercrime, using qualitative interviews from our recent study exploring older people's experiences of cybercrime in Mumbai.

BACKGROUND

As global internet penetration increases, so does cybercrime. The estimates for money lost by individuals and businesses to online fraud range from a 100 billion to a trillion dollars a year (Hyman, 2013). While determining the societal cost of this crime presents challenges (Furnell, Emm and Papadaki, 2015), experts agree that a brunt of this loss is borne by ordinary, home or novice internet users (Solms, 2010; Furnell, Tsanagidi and Phippen, 2008). There has been global, rapid growth in the number of people aged over 60 (Wagner, Hassanein and Head, 2010). Older adults are a fast growing group of internet users (Hart, Chaparro and Halcomb, 2008), using the internet for banking, shopping, 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 (Carlson, 2006). Although fraud affects people of all ages (DeLiema, 2017), older adults are disproportionately vulnerable (Kirchheimer, 2011; Shao et al., 2019). The few studies that have sought to understand why and how older adults are vulnerable to cybercrime took place in higher income countries. In these studies, older people were found to be attractive targets to criminals due to their perceived relative lack of familiarity with technology, relative wealth and hesitancy to report the crime to authorities due to feelings of shame (Burnes et al., 2017; Button, Lewis, & Tapley, 2014; Han et al.2016). Financial victimization often had a devastating impact on older people's wellbeing, leading to physical and emotional ill-health, loss of trust, feelings of shame, and social withdrawal (Burnes et al., 2017; Button, Lewis, & Tapley, 2014; Han et al., 2016).

Internet use among older Indian people

India is a Lower Middle Income Country (LMIC) with the world's second largest older adult population, which is projected to grow to 179 million in 2031 and then 327 million in 2050 (Rajan, Sarma and Mishra, 2003). India's rapidly growing economy is bringing more people online especially in its metropolitan cities where there is an increased penetration of

broadband and internet services (The Economic Times, 2018). Much like their younger counterparts, older people rely on their smartphones to access the internet.

The majority of older internet users in India live in urban areas with good connectivity at affordable rates (Sharma et al., 2015). Older Indian men use online technology more than older Indian women, probably due to relatively high literacy rates in older urban men (The Economic Times, 2018). In a survey of 500 older urban internet users in India, respondents indicated that they used the internet to connect with family and friends and for online shopping (The Economic Times, 2016).

Cybercrime and older people in India

Increased urbanization and the breakdown of the joint family are purported to have left this growing population vulnerable to abuse, including financial victimization (Chokkanathan, Natarajan and Mohanty, 2011; Government of Tamil Nadu, 2003; Ingle & Nath, 2008; National Sample Survey Organization, 2006). The Indian government does not publish specific data on cybercrime incidents perpetrated against older victims, as it does for other crimes. The most common crime against older people, both country-wide and in Mumbai, in 2016 was that of cheating and fraud registered under of section 420 of the Indian Penal Code (Risbud, 2016). This reflects the general understanding in criminological studies that older people are particularly vulnerable to fraud (Carlson, 2006), and this probably includes fraud perpetrated online. Mumbai is an attractive target for cybercriminals because it is the financial capital of India with a prosperous middle class (Risbud, 2016). Government crime statistics record that in 2016 more cybercrime cases were recorded in Mumbai than any other large city (NCRB, 2016). As in other parts of the world, cybercrime is probably very significantly under-reported (Tcherni et al., 2016).

Exploring cybercrime in Mumbai: using a Crime Triangle framework

In 2017, we interviewed six Mumbai residents aged 60 and over who had been victims of cybercrime, and five of their family members. The victims interviewed were all males, aged from 62 to 77 years, graduates and used the internet for an average of an hour a day before their victimisation. They lost between 30K and 2000K rupees, through cell phone, bank card hacking or social engineering fraud. We also interviewed seven experts: two from banking (n=2, a Bank Chairman and Chief technology office), one police inspector, one lawyer, one private investigator specialising in cybercrime and two older people's welfare workers from a third sector organisation. The first author recruited professionals through local contacts, and people who were victims of cybercrime and their family members through the professionals interviewed. Our aim was to gain a rich understanding of the experiences of older people in Mumbai who have experienced and reported cybercrime.

The first and second author carried out semi-structured, qualitative interviews, in English or Hindi. The interview topic guide for victims and family members encompassed how the cybercrime took place, experiences reporting the crime, impacts of the crime upon victims, their emotional and practical responses; and how the crime might, from the perspectives of interviewees, be prevented, or better managed. Participating professionals were asked if, how and why older people might be particularly vulnerable to cybercrime, what they consider to be protective factors, and about the institutional response to cybercrime experienced by older people in Mumbai and how it might be prevented or better managed.

In order to explore how the older people, and people who supported older people, understood why they had become victims of cybercrime, what factors had made this more likely and what they considered might have prevented, we used a theoretical thematic framework approach. This is driven by the researcher's theoretical or analytical interest in the area, and is thus more

explicitly analyst-driven technique than other qualitative analysis techniques. Our theoretical basis was the crime triangle approach (Felson and Cohen, 2008). This has been used to understand the occurrence of cybercrimes (Leukfeldt and Yar, 2016; Newman, 2009). It states that the successful completion of any crime requires three elements:

1. Lack of a guardian to protect the target from the offender

2. A suitable target

3. A motivated offender.

FIGURE 1 GOES HERE

Further details of study methodology are available from the authors. We describe findings from our qualitative analysis below, and discuss them in the context of previous literature.

1. "LACK OF GUARDIANSHIP"

Unresponsive institutions

The older cybercrime victims we interviewed described institutional barriers to reporting crimes, and failures of banks and the police to protect victims. There was a strong sense in participant's narratives that local banking and police systems were unresponsive and challenging for users to navigate. The participants who had been victims of cybercrime described long delays before they could register alleged crimes with police.

"In foreign countries if anything happens the bank will take the responsibility and refund the money, here bank will not take any cognisance of it."

(Wife of a victim)

"*Senior inspector said he will lodge the complaint but he didn't adhere to it. Then I approached the higher officer that is Assistant Police Commissioner, and because of him he lodged a complaint…but after one month. He used to tell me I don't have time. Sometimes he never used to take my call. So after six to seven months, he has given me the complaint copy."*

(Victim of a cybercrime)

"One of the problems that we faced was that when these kind of phishing, wishing attacks increased the police at some stage were taking a stand that since so many instances were getting reported they said they will not be able to respond to them."

(Chairman of a bank)

"We went to the police station with the details that the bank gave us. So they said, Sir, you are not the first one to come in, you know, you've just lost around 30,000 we've got cases of like 50,000 pending and this normally happens with senior citizens."

(Daughter of a victim)

Our findings mirror Chokkanathan, Natarajan and Mohanty's (2011) study in Chennai where participants reported lack of accessibility and trust in police as reasons for not reporting abuse by their family members. This lack of responsiveness could be the consequence of a low police to public ratio (NCRB, 2016). Police are often overburdened with work and lack the resources and sometimes technical skills to respond to every complaint of cybercrime.

Lack of data protection and privacy safeguards

The victims all reported that unauthorised transfers of their personal information to criminals by banks and telephone companies facilitated crimes.

"I don't know how my bank card and account number went to that person. They told me my bank card number, name of the bank and bank account number. Either they are in cahoots with the bank people, or getting it from somewhere else. And bank is of no help to us, to senior citizens, nothing, no help."

(Victim of a cybercrime)

"Where this country probably is behind the rest of the world is in customer privacy and the data protection standards. I don't think we still have a definite law in that. I would concede that the kind of consumer protection that we have in this country needs to go a long way to reach the kind of levels that is available in some of the western countries"

(Chairman of a bank)

There appeared to be a lack of a clear legal framework on data protection and privacy and of a regulatory insurance framework to make banks liable for losses of their customers and compensate them for fraud attributable to weaknesses in the banks' security systems. None of the participants who were interviewed had recovered the entire amount they lost to cybercrime. Narratives were consistent with the well-recognised strategy of "responsibilization" of the victims (Walkgate, 2006) where they were blamed for their own loss. This has been reported to prolong and exacerbate victim experiences of stress, feelings of depression and sense of shame (Cross, 2007).

2. "SUITABLE TARGET"

Participants felt that older people in Mumbai were less heard than younger people. Ageist attitudes and stigma were blamed for a belief that police and banks and their crimes were not taken seriously.

> *The banks, they would be more cautious when if it's a youngster because they know that the guy knows technology, that the guy can approach the police and can become a pain for the police people and can become a pain for the bank also. He can go onto social media and talk and just express his disgust and anger online.*

(Cybercrime private investigator)

Unfamiliarity with security precautions when using technology for online financial transactions was described by several interviewees (but not by victims themselves) as increasing older people's vulnerability to cybercrime. Several interviewees considered that adapting to new technology was more challenging for older people, and that they were inadequately supported to make this change.

> "*Nowadays when our government is forcing us, they are leading us to make Digital India. Okay, you make digital India but what about the old people? You make them being expected compulsory to use smartphone, so you're ready for giving the benefits to the smartphone companies, and what will happen to the older people? They use smartphone does not mean that they are smart enough to use it for online transactions. And not they are guarded against being victims.*"

(Wife of a victim)

> "*Senior citizens don't understand that they have to protect their password very carefully. Since it is very difficult, maybe it is difficult for them to remember the password, they write it somewhere... They*

generally write it on a paper and keep it with the credit card or the debit card. So if their wallet is stolen, then all the information is gone."

(Police inspector)

Lack of proximal family support

Professionals and family members interviewed described an urban, Indian, middle class for whom success often meant children living in a higher income country. Having family abroad is a frequent reason for older people accessing the internet, yet this increased familiarity with an online world could potentially increase vulnerability to cybercrime.

Four of the six victims interviewed either lived alone or had children who had moved abroad for employment. Several interviewees who were not themselves victims of cybercrime considered that proximal support of younger family members might help prevent cybercrime where this is available:

"The senior citizens themselves are alone. Like I know so many who are just alone. They are just staying there. They're happy that their children are reaping good benefits in the United States or Australia or London, wherever it is. So it gets difficult for them because they are confused. They don't know. And if the police suddenly says go, get the IP of this. He says what is this IP. He doesn't know what is an IP."

(Cybercrime private investigator)

"… loneliness, isolation, these are the feelings that make them want to develop a bond between even a stranger because if a stranger is ready to listen to them, you know, and try to build that kind of sense of trust."

(Member of charity organisation)

Relative affluence

Relative affluence of older people compared with younger people in Mumbai was cited by two professionals interviewed as a possible vulnerability factor:

"In Mumbai the elderly get targeted largely because Mumbai is relatively a prosperous city in this country, the elderly are people who will have more of a more healthy cash balance or whatever so these

are richer people by margins, and hence I think there is definitely a target on them."

(Bank CTO)

3. "MOTIVATED OFFENDER"

The professionals interviewed described the criminals targeting older people as organised and rarely prosecuted which made it a low risk, high reward crime.

"The criminals are organised. If some amount is stolen or deposited by some victim in an account here in Bombay, the amount is withdrawn from different ATMs all over India. And it has to be an organised racket to work in this fashion. Moreover, it is a very low-risk crime. Even if the criminal is caught, there is no proper investigation to collect the evidence and to take the case to its logical end. That's why the criminals have become more and more bold to commit these type of crimes."

(Police inspector)

This view is supported by figures compiled by the Mumbai Police. The official data showed that an arrest was made by the police in only 841 of the 4,212 cybercrime cases registered between January 2014 and March 2018. The rate of detection of crime was even lower in cases of bank card fraud where only 11% of the 1,532 cases were solved, and only 5% of the total money lost to cybercriminals was recovered (Narayan, 2018). These numbers represent only the cases reported to the police, a fraction of actual victimisations (Bidgoli and Grossklags, 2016).

IMPACT OF CYBERCRIME ON OLDER PEOPLE

The crime had a profound impact on the older victims interviewed. The money they lost was part of their life savings and put aside for emergencies like medical treatments. Some interviewees felt that police officers and banks considered older victims' cases to be of low priority because they perceived the amount lost to be relatively low. The victims experienced losing savings to fraud after their retirement as a blow to their financial stability and urged the authorities to take it seriously. Fraud can be more debilitating on older victims as they cannot recoup their losses by returning to the job market like younger adults (Rabiner, Brown and O'Keefe, 2004).

The crimes led to persistent and unresolved feelings of shame, depression and anxiety.

> *"You feel very depressed when you tell anybody else that this thing has happened with me, my money has been stolen…First thing when you are old the age is the thing that makes you victim of everything. So you feel very sad, because you cannot save yourself from such criminals. These are unknown things you have to face."*

(Victim of a cybercrime)

This was consistent with findings from studies on traditional forms of fraud (Jingjin Shao et al., 2019; Burnes et al., 2017; Button, Lewis, & Tapley, 2014; Han, Boyle, James, Yu, & Bennett, 2016).

The crimes left older victims wary of new technology and to partial or complete withdrawal from using the internet, online banking or making cashless transactions.

> *"Losing an amount of nearly 45,000 Rupees is not a small thing. I was scared to deal with credit cards. Now I don't do any online payments."*
> **(Victim of a cybercrime)**

> *"Now I am fully stressed in my mind, he is also fully stressed. I don't want credit card, I don't want debit card. Because I'm not at all sure that any bank is secure, and they have proper security. So I just want to keep away from that. Even if the banks try to force us we'll go by our old faithful method and pay by cheque."*

(Wife of a victim)

This is a cause of concern for the government and policy makers who are working towards the goal of a Digital India (Ministry of Electronics and Information Technology, 2019). Older people may be left behind in this initiative, if their fears of online security are not addressed.

CONCLUSIONS

In this brief report, we describe possible vulnerability factors for cybercrime among older people in Mumbai, as well as the potential impact of this crime. We draw on the limited, existing literature on cybercrime and older people in LMIC and use our qualitative interviews with older people who have been victims of cybercrime in Mumbai and their supporters to illustrate and add to these findings. The sample size was small but suitably diverse for the first exploratory

study of this nature. It was difficult for the researchers to recruit participants without convenience sampling in near total absence of official data on the subject. However, the final sample included victims of three most common types of cybercrime in Mumbai and their relatives. The experts interviewed represented the views of the major institutions—police, the legal system, investigators and Non-governmental organisations—who interact with older people who are victims of cybercrime.

The perspectives we present highlights the importance of data protection in preventing online fraud, the need to provide older people, who constitute a high risk group, with the skills, awareness and tools to take precautions in sharing their private information and training of frontline staff in banks, phone companies and police stations on how to avoid data leaks and support victims when crimes occur. These preliminary findings can inform larger studies to support the design of safeguards for older, internet users in LMIC; as well as training for staff of banks and police on how to respond to older people reporting cybercrime.

References:

Bidgoli M, Grossklags J. (2016) End user cybercrime reporting: what we know and what we can do to improve it. In Cybercrime and Computer Forensic (ICCCF), IEEE International Conference on 2016 Jun 12 (pp. 1-6). IEEE.

Burnes, D., Henderson Jr, C. R., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (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., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36-54.

Carlson, E.L. (2006). Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow. Elder LJ.14:423.

Chokkanathan, S., Natarajan, A., & Mohanty, J. (2014). Elder abuse and barriers to help seeking in Chennai, India: A qualitative study. *Journal of elder abuse & neglect*, *26*(1), 60-79.

Cross C. (2015). No laughing matter: Blaming the victim of online fraud. International Review of Victimology. 2015 May;21(2):187-204.

DeLiema, M. (2017). Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist*, *58*(4), 706-718.

Felson M, Cohen L. (2008). Routine activity theory. Environmental Criminology and Crime Analysis. Cullompton, UK: Willan Publishing.70-7.

Furnell S, Emm D, Papadaki M. (2015). The challenge of measuring cyber-dependent crimes. Computer Fraud & Security. Oct 1, 2015(10):5-12.

Furnell S, Tsaganidi V, Phippen A. (2008). Security beliefs and barriers for novice Internet users. Computers & Security. 2008 Dec 1;27(7-8):235-40.

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

Hart T.A., Chaparro BS, Halcomb CG. (2008). Evaluating websites for older adults: adherence to 'senior-friendly' guidelines and end-user performance. Behaviour & Information Technology. May 1, 2008 ;27(3):191-9.

Hyman P. Cybercrime (2013) : it's serious, but exactly how serious? Communications of the ACM. 2013 Mar 1;56(3):18-20.

Kirchheimer, S. (2011). Scams trap older adults. *AARP Bulletin*, *1*.

Leukfeldt ER, Yar M. (2016) Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior. 2016 Mar 3;37(3):263-80.

Ministry of Electronics & Information Technology, Government of India. Digital India. http://digitalindia.gov.in/

Ministry of Statistics and Programme Implementation. (2016) Elderly in India.

Narayan N. (2014) Only one in five cases of cybercrime solved in Mumbai in 4 Years. The Times of India. 2018 May 14. Also at: https://timesofindia.indiatimes.com/city/mumbai/only-one-in-5-cases-of-cyber-crime-in-mum-solved-in-4-yrs/articleshow/64152462.cms

National Crime Records Bureau. Crime in India. (2016). Also at: http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf

Newman G.R. Cybercrime. (2009) In Handbook on crime and deviance (pp. 551-584). Springer, New York, NY.

Rabiner, D. J., O'Keeffe, J., & Brown, D. (2006). Financial exploitation of older persons: challenges and opportunities to identify, prevent, and address it in the United States. *Journal of aging & social policy*, *18*(2), 47-68.

Rajan, S. I., Sarma, P. S., & Mishra, U. S. (2003). Demography of Indian aging, 2001-2051. *Journal of aging & social policy*, *15*(2-3), 11-30.

Risbud N. (2014) Mumbai, India.

Shao, J., Du, W., Lin, T., Li, X., Li, J., & Lei, H. (2019). Credulity rather than general trust may increase vulnerability to fraud in older adults: a moderated mediation model. *Journal of elder abuse & neglect*, 1-17.

Sharma A, Kaur M, Koradia Z, Nishant R, Pandit S, Raman A, Seth A. (2015) Revisiting the state of cellular data connectivity in India. In Proceedings of the 2015 Annual Symposium on Computing for Development 2015 Dec 1 (pp. 149-157). ACM.

Tcherni M, Davies A, Lopes G, Lizotte A. (2016) The dark figure of online property crime: is cyberspace hiding a crime wave?. Justice Quarterly. 2016 Jul 28;33(5):890-911.

The Economic Times. (2016) Here's why senior citizens are becoming heavy e-commerce & social media users. 2016 Nov 1. Also at:

https://tech.economictimes.indiatimes.com/news/internet/how-senior-citizens-are-becoming-heavy-e-commerce-users/55257833?redirect=1

The Economic Times. (2018) Internet users in India expected to reach 500 million by June: IAMAI. 2018 Feb 20. Also at: https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-expected-to-reach-500-million-by-june-iamai/articleshow/63000198.cms

Wagner N, Hassanein K, Head M. (2010) Computer use by older adults: A multi-disciplinary review. Computers in human behavior. 2010 Sep 1;26(5):870-82.

Walklate S. (2006) Imagining the victim of crime. McGraw-Hill Education (UK)