Mass Marketing Fraud

Morgane Coat, Master's candidate

Briefing Note
Vol. 1 Iss. 4

RCCP | Research Chair in Cybercrime Prevention

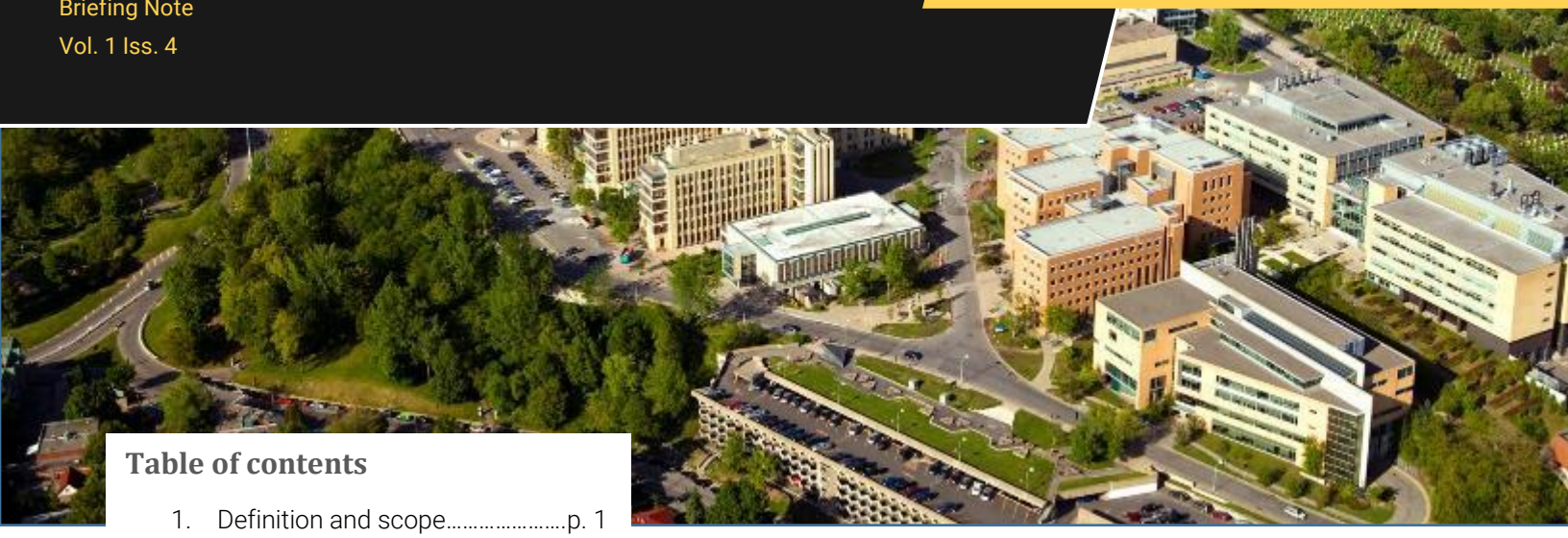

Table of contents

The Research Chair in Cybercrime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Bank of Canada. Led by Benoît Dupont, researcher at the International Centre for Comparative Criminology at the University of Montreal, its mission is to contribute to the advancement of research on cybercrime phenomena from the perspective of its prevention.

Definition and Scope

Mass marketing fraud is defined as "**any false, deceptive, misleading or fraudulent act intended to get you to send money or provide personal information. This includes unsolicited requests or offers received through the telephone, mail, internet or email, and door-to-door campaigns**".[1] In Canada, in 2018, mass marketing fraud cost victims nearly $**100 million, including $55 million online.**[2]

Victim profile

- Typically, **men** are more likely to fall victim to fraud.[3] [4] [5]
- People **aged 18 to 24 are most likely to send their personal data** in response to a fraudulent request.
- **People aged 65 and over are more likely to send money** than other age groups.
- People **aged 35 to 44 are the least likely** to send money in response to a fraudulent request.[6]

Risk Factors

Fraud victims have been shown to make several **motivational and cognitive errors of judgment** in their decision-making, including:[7 8 9 10]

- Placing greater trust in individuals whom they consider to be **authority figures**.[10]
- Being more sensitive to **"visceral triggers"** often used by fraudsters.[10] Fraudsters use these triggers—which include money, sex, love, pain and sorrow—to turn victims' attention toward the benefits, that is, to some imagined positive emotional state they could experience in the future.
- **Making decisions faster** when presented with time-sensitive or rare opportunities.
- **Lacking self-control**.
- Being **overconfident** and overestimating their ability to identify potential fraud, since they believe they know enough about the problem to avoid it.[7 10 11] This is because the more knowledgeable a person is in a given area, the more skilled they feel in it, thereby overestimating their ability to make good decisions.
- **Thrill-seeking**.

Victims may also be more likely to fall for **some techniques used by fraudsters**, such as pressure, coercion and making the victim believe that they have things in common.[7 10]

Cyber fraud victims are more likely to **be impulsive** when faced with urgent situations or thrilling opportunities. They're also more likely to struggle with **dependency issues (drug, game, etc.)** or to engage in **risky online behaviour**, including making purchases on foreign websites, online gaming, participating in online discussion forums and dating sites and spending on pornography.[12 13 14]

Some victims often use **more cognitive effort** and spend more time assessing whether they're being frauded than non-victims. This may be because victims may not necessarily know **how to differentiate** legitimate offers from fraudulent ones.[7 12 15]

This apparently contradicts the fact that impulsive individuals are also more likely to fall victim to fraud, but that may be because some impulsive individuals may actually delete an offer or an email without paying too much attention to it.[7] Impulsiveness may therefore affect one's likelihood of falling victim to fraud in 2 different ways.

People with **higher levels of education**, those who think they have **more control over external events**, and those who tend to **act with forethought** are also more likely to be cyber fraud victims.[12]

Fraud victims tend **not to talk to their friends and relatives** about ongoing scams or scams they've fallen victim to in the past.[16]

The money victims lose to fraud mainly comes from their **personal savings**; however, some victims go as far as taking out personal loans, borrowing money from friends and relatives and mortgaging assets.[9 17]

Certain victims also find it very **hard to believe** that they are being scammed and may **continue falling for it**, even after authority figures (police, the bank, etc.) point out what's really going on.[9 16]

Between **26% and 45% of cyber fraud victims** will be defrauded again **at least once in their lifetime**. However, there appears to be no real distinction between one-off and repeat victims.[9 18] The difference between these 2 types of victims may be explained by different levels of gullibility.[7]

Some **more psychological theories and findings** may also explain why certain people fall victim to scams more easily:[7 9]

- The **sunk cost effect** (also called the near-miss phenomenon): Victims who have already invested money in a scam once, or

who consider that they have already invested considerably, think that by continuing to invest a little more, they will get closer to their goal and end up reaching it. The near-miss phenomenon may possibly explain victims' dependence on scams and why they find it so tough to disengage from them.

- Gambling: Even if an offer doesn't seem reliable, given the potential gains, victims are persuaded to try their luck; they think it's worth the trouble considering the offer may ultimately turn out to be legitimate.

Recommendations

It's important to raise awareness about this issue and educate people so that they can learn how to detect fraud and recognize the various persuasion techniques fraudsters use.[16] [19] Education and awareness campaigns should apply general and targeted approaches based on participants' age, lifestyle (that is, whether they engage in at-risk activities) and the type of technology they use.[6] [7] [20]

Predictive modelling of cybercrime victimization and any approach used to prevent fraud victimization must take into account the full range of victims' characteristics, including socio-demographic and psychological characteristics, personality traits, online activities[12] [20] and their various motivational and cognitive processes.[7]

Since knowing how to recognize a scam doesn't necessarily prevent you from falling victim to one, we should develop initiatives other than those centred on education and raising awareness, and go beyond simply teaching people how to detect fraud.[9] [18]

Study limitations

The above-mentioned studies do not necessarily distinguish between online and offline fraud.

Given the high level of shortcomings, contradictions and unclear information in the studies' findings, further research is needed to gain a better understanding of why some people fall victim to fraud more easily than others.

References

1. Canadian Anti-Fraud Centre. (2019). *Mass Marketing Fraud: Recognize, Reject and Report it! Scam Digest: Ask us about fraud: A guide to recognizing and avoiding mass marketing fraud*. First Canadian Edition.

2. Canadian Anti-Fraud Centre. (2019). Unpublished data.

3. Anderson. K. B. (2016). Mass-Market Consumer Fraud: Who is Most Susceptible to Becoming a Victim*? FTC Bureau of Economics*, *332*.

4. Mesch, G. S. and Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356-1371.

5. van de Weijer, S. G. A. and Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, *20*(7), 407-412.

6. Jorna P. (2016). The relationship between age and consumer fraud victimisation. *Trends and Issues in Crime and Criminal Justice*, *519*(2016), 1-16.

7. Lea, S. E. G, Fischer, P. and Evans, K. M. (2009a), 'The Psychology of Scams: Provoking and Committing Errors of Judgement'. *Office of Fair Trading*.

8. Lea, S. E. G., Fisher, P. and Evans. K. M. (2009b), 'The Economic Psychology of Scams', *International Association for Research in Economic Psychology and the Society for the Advancement of Behavioral Economics*.

9. Whitty, M. (2013). The Scammers Persuasive Techniques Model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology*, *53*(4), 665–684.

10. Button, M., Nichols McNaughton, C., Kerr, J. and Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, *47*(3), 391-408.

11. Jansen, J. and Leukfeldt, E. R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

12. Whitty, M. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277-292.

13. Chen, H. Beaudoin, C. E. and Hong. T (2017). Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior*, *70*, 291-302

14. Gainsbury, S. M., Browne, M., and Rockloff. M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society*, *21*(6), 1232-1252.

15. Downs, J. S. Holbrook, M. B. and Cranor. L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, 79-90.

16. Oliver, S., Burls, T., Fenge, L.-A., and Brown, K. (2015). "Winning and losing": vulnerability to mass marketing fraud. *Journal of Adult Protection*, *17*(6), 360–370.

17. Ross, S. and Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice*, *420*(2011), 1-6, 1. In this latest study, researchers found that 80% of their participants used their personal savings when being scammed, 13% took out a loan, 10% had borrowed from their relatives and 5% had mortgaged their assets.

18. Whitty, M. (2015). "Mass-marketing fraud: a growing concern". *IEEE Security and Privacy*, *13*(4), 84-87.

19. Sofo, F., Berzins, M., Ammirato, S., and Volpenstesta, A. (2010). Investigating the relationship between consumers' style of thinking and online victimization in scamming. *International Journal of Digital Content Technology and its Applications*, *4*(7), 38-49.

20. Norris, G., Brookes, A. and Dowell. D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3), 1-15