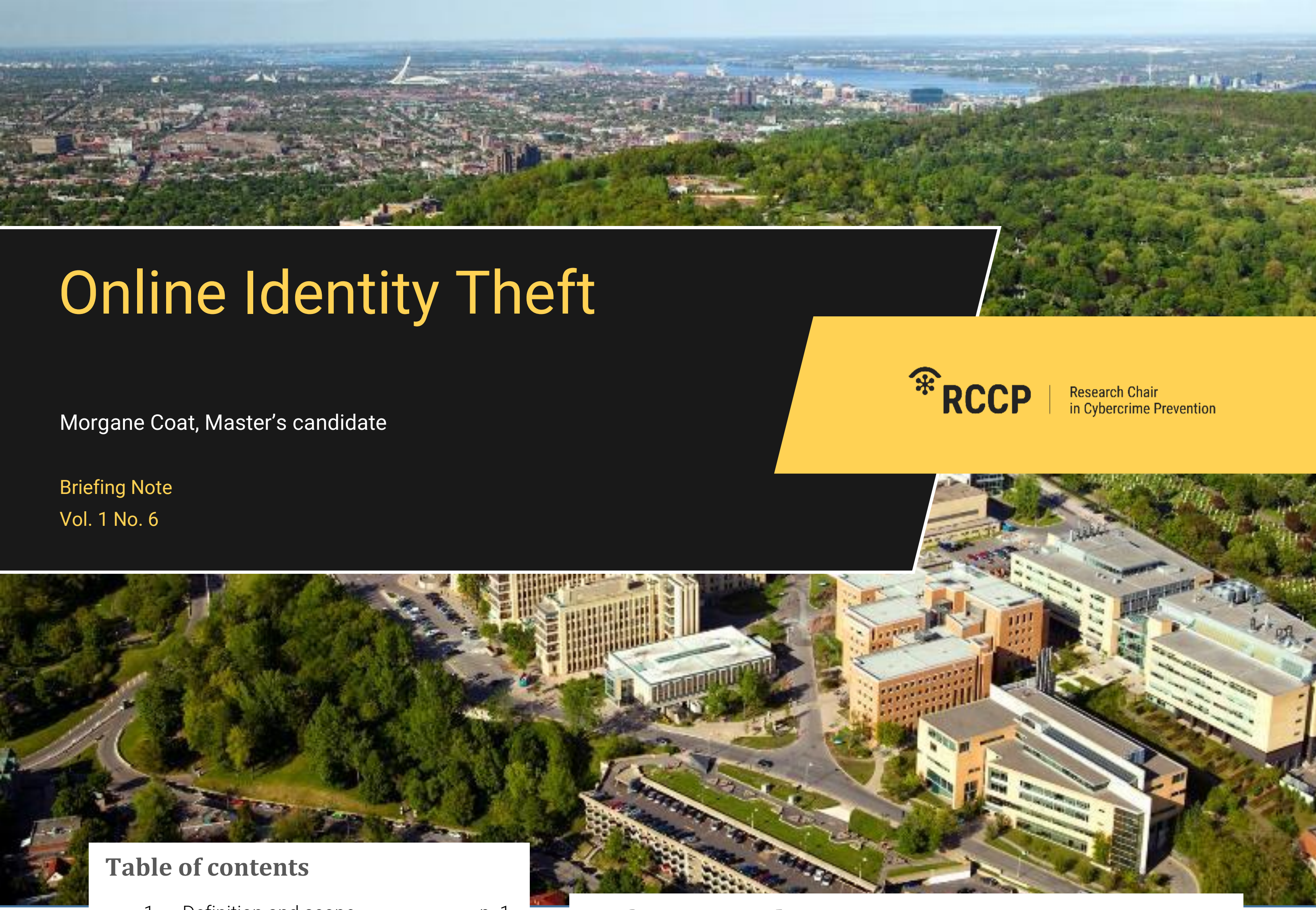

Online Identity Theft

RCCP | Research Chair in Cybercrime Prevention

Morgane Coat, Master's candidate

Briefing Note
Vol. 1 No. 6

Table of contents

The Research Chair in Cybercrime Prevention was created on the initiative of the University of Montreal, Desjardins and the National Ban k of Canada. Led by Benoît Dupont, researcher at the International Centr e 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

Identity theft is the **acquisition and collection of another person's personal information for criminal purposes.**[1] The criminal's goal is to **impersonate their victim** for their own benefit.[2] [3] They target information such as **credit card and bank account numbers**, **full names**, **signatures**, **dates of birth**, **social insurance numbers**, **mothers' maiden names, logins, passwords** and **driver's licence and passport numbers.**[4] To get this information online, fraudsters use **spyware**, **viruses**, **hacking** or **phishing**.[5] They can then use this stolen personal or financial data **to access a computer, email account or bank account, open bank accounts, apply for credit cards, make purchases or receive government benefits**. In 2018, this type of fraud was reported **122 times** in Canada and resulted in nearly **$18,000 in losses**.[6]

Victim profile

Given the widely contradicting claims in the literature, it would appear that **there are no specific socio-demographic characteristics that define fraud victims**. That means that **anyone, regardless of where they're from, their socio-economic status, their education, gender or age** could be a victim of online identity theft.[7] [8] [9] [10]

Risk factors

Individuals who display risky behaviours online or engage in cybercrime—such as using, making or sharing pirated software or media, using another person's wireless Internet connection without their authorization or accessing another person's documents and information without their knowledge—are more likely to fall victim to identity theft.[9]

Research has shown that many online activities, such as auctions, banking and online shopping, increase the risk of identity theft.[11] [12] However, this could be explained not by the fact that these activities are inherently risky, but rather because the victim and thief can end up on the same Wi-Fi network (for example, an unsecured public Wi-Fi network).[7]

This risk further increases for former hacking or phishing victims or people whose personal information has been made public.[10] [12] People who are more afraid or who believe they're more at risk of becoming online identity theft victims are more likely to be targeted.[8] [10] In fact, people who have been victims of this type of fraud before may believe they have a higher chance of being targeted again.

Accessing the Internet through university or public computers also increases people's risk of falling victim to identity theft.[11]

Protective factors

Using secure browsers and regularly updated protection software, such as anti-virus software, anti-spyware and ad blockers, are important protective and resilience factors in mitigating identity theft risk.[9] [11]

It has also been shown that the more someone knows about phishing, identity theft and anti-phishing technologies, the likelier they are to use anti-phishing technologies to protect themselves from identity theft or other cyber threats.[7]

Recommendations

Financial institutions and various businesses that store personal information should further raise awareness of the risks associated with phishing, online identity theft and personal information protection on the Internet. They should also help teach people how they can protect themselves.[7]

Given the wide range of online activities correlated with a higher risk of becoming a victim of online identity theft, people should be made more aware of how to use the Internet and different networks safely (for example, how to use public Wi-Fi connections safely), and which online activities can be potentially risky.[8]

Study limitations

The few studies that focus on online identity theft victimization rely primarily on Cohen and Felson's routine activity theory, which states that three factors must converge for victimization to occur: a motivated offender, an accessible target and the absence of capable guardians. It may therefore be useful to explore how other theories can help us understand online identity theft.

Studies to date have only focused on risky online activities, the use of computer devices and the lack of security measures like anti-virus software to explain online identity theft victimization. At this time, no study seems to have focused on the victims' cognitive or personality traits (like impulsivity).

References

[1] Canadian Anti-Fraud Centre. (CAFC). (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] Better Business Bureau. (BBB). (2019). *Tech-Savvy Scammers Work to Con More Victims: 2018 BBB Scam Tracker Risk Report*. BBB Institute for Marketplace Trust.

[3] Not to be confused with identity fraud, which is more about impersonating someone without committing identity theft (the deceptive use of another person's identity information for the purpose of committing various acts of fraud). (Canadian Anti-Fraud Centre. [2018]. *Identity theft and identity fraud*).

[4] Canadian Anti-Fraud Centre. (2018). *Vol d'identité et fraude à l'identité*.

[5] Competition Bureau Canada. (2012). *Le petit livre noir de la fraude*.

[6] Canadian Anti-Fraud Centre (2019). Unpublished data.

[7] Cornelius, D. R. (2016). Online identity theft victimization: An assessment of victims and non-victims level of cyber security knowledge (Doctoral dissertation, Colorado Technical University).

[8] Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238.

[9] Holt, T. J. and Turner. M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, *33*(4), 308-323.

[10] Paek, S. Y. and Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626-642.

[11] Williams, M. L. (2016). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48.

[12] Reyns, B. W. and Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-113.