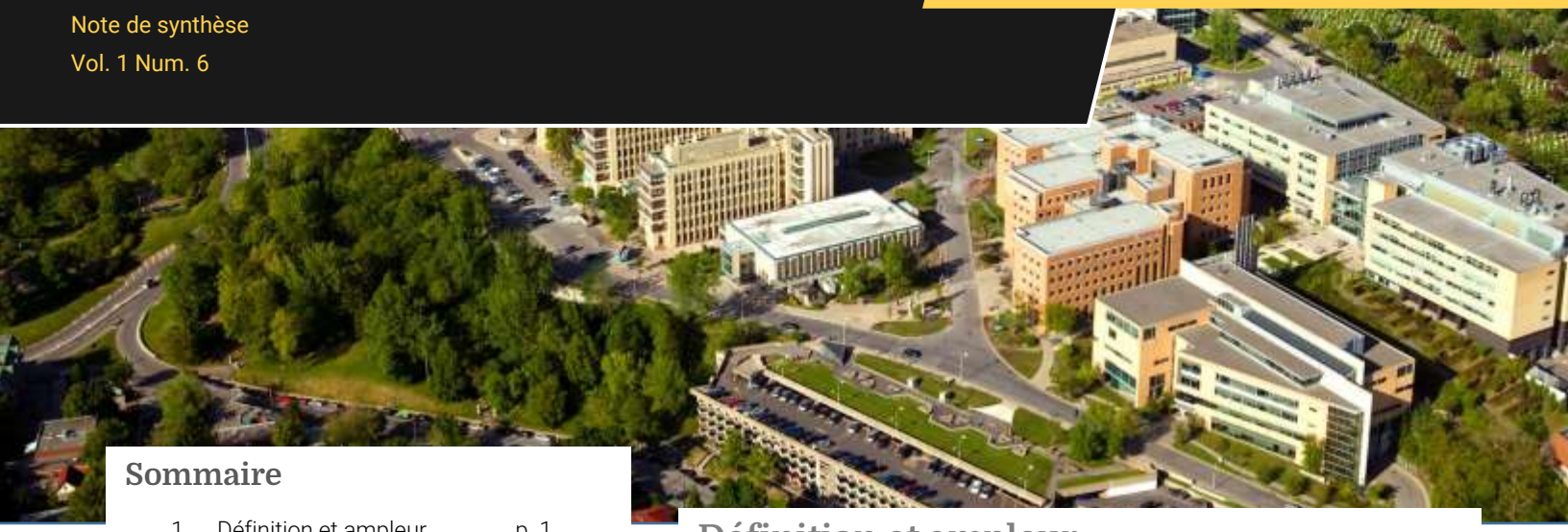
Le vol d'identité en ligne

Morgane Coat, candidate à la maîtrise

Note de synthèse
Vol. 1 Num. 6

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

La Chaire de recherche en prévention de la cybercriminalité, créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada; et dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Définition et ampleur

Le vol d'identité désigne **l'acquisition et la collecte de renseignements personnels d'une autre personne à des fins criminelles**[1], dans le but **de se faire passer pour cette personne** à son propre avantage[2 3]. Les fraudeurs ciblent les renseignements tels que les **numéros de carte de crédit et de comptes bancaires**, le **nom complet, la signature**, la **date de naissance**, le **numéro d'assurance sociale**, le **nom de jeune fille de la mère**, les **identifiants en ligne et mots de passe**, les **numéros de permis de conduire et de passeport**[4]. Pour obtenir ces renseignements en ligne, les fraudeurs peuvent avoir recours à des **logiciels espions**, des **virus**, du **piratage** ou de **l'hameçonnage**[5]. Les criminels peuvent utiliser ces données personnelles ou financières volées pour **accéder à un ordinateur et à un compte de courriel**, **accéder à des comptes bancaires** ou **en ouvrir de nouveaux**, **faire des demandes de cartes de crédit**, **faire des achats** ou **toucher des prestations gouvernementales**. En 2018, au Canada, cette fraude a occasionné près de **18 000 dollars de pertes** pour **122 signalements**[6].

Profil des victimes

Considérant les nombreuses contradictions au sein de la littérature, il semblerait qu'**il n'existe pas de caractéristiques sociodémographiques particulières des victimes de cette fraude**. Ainsi, **toute personne, quel que soit son origine, son statut socioéconomique, son niveau de scolarité, son sexe ou son âge** peut être victime d'une telle fraude[7 8 9 10].

Facteurs de risque

Les personnes qui adoptent des **comportements à risque en ligne** ou qui **participent à des activités cybercriminelles** telles que l'utilisation, la fabrication ou le partage de logiciels ou de médias piratés, le fait d'accéder aux documents et renseignements d'une autre personne à son insu ou de chercher à deviner son mot de passe, et le fait d'utiliser une connexion internet sans fil d'une autre personne sans son autorisation sont **plus susceptibles d'être victimes de vol d'identité**[9].

Il a été démontré que **de nombreuses activités en ligne** comme la **vente aux enchères**, **l'utilisation de services bancaires** et **les achats en ligne** augmentent le risque d'être victime de vol d'identité[11] [12]. Toutefois, cela pourrait s'expliquer non pas par le fait que ces activités soient risquées en tant que telles, mais davantage **parce que la victime et le voleur peuvent se retrouver sur un même réseau Wi-Fi** (par exemple, un réseau Wi-Fi public non sécurisé)[7].

Avoir des renseignements personnels ayant été rendus publics, ou encore **avoir été victime de piratage informatique ou d'hameçonnage** augmente également le risque[10] [12]. Les personnes **qui ont plus peur ou qui perçoivent un risque plus élevé** de devenir victime de vol d'identité en ligne **sont plus susceptibles de le devenir**[8] [10]. En effet, il est possible que les individus perçoivent un risque plus élevé de victimisation parce qu'ils ont déjà été victime de cette fraude auparavant.

L'accès à Internet via des ordinateurs universitaires ou publics augmente également le risque de victimisation[11].

Facteurs de protection

L'utilisation de navigateurs sécurisés et de logiciels de protection mis à jour régulièrement tels que les logiciels anti-virus, les anti-espiogiciels et les logiciels anti-publicitaires agissent comme des **facteurs de protection et de résilience** importants face au risque de vol d'identité[9] [11].

Il a également été démontré que **plus un individu à de connaissances élevées concernant l'hameçonnage, le vol d'identité et les technologies anti-hameçonnage**, **plus son intention d'utiliser ces technologies pour se protéger du vol d'identité ou des autres cybermenaces augmente**[7].

Recommandations

Les institutions financières et les diverses entreprises possédant des renseignements personnels devraient davantage **sensibiliser les individus sur les risques liés à l'hameçonnage, au vol d'identité en ligne, à la protection des renseignements personnels sur internet, ainsi que sur la manière dont les individus peuvent se protéger**[7].

Considérant la **large gamme d'activités en ligne corrélées à un risque plus élevé de devenir victime** de vol d'identité en ligne, les individus devraient être **davantage sensibilisés à l'utilisation sécurisée d'internet et des réseaux** (accès à internet via une connexion wifi publique par exemple), en plus des activités en ligne qui pourraient s'avérer risquées[8].

Limites des études

Les quelques études qui se sont attardées sur la victimisation au vol d'identité en ligne se sont principalement appuyées sur la **théorie des activités routinières de Cohen et Felson** qui stipule que la victimisation résulte de la rencontre entre un **délinquant motivé**, une **cible accessible** et une **absence de gardiens**. D'autres théories pourraient ainsi être davantage sollicitées pour comprendre le vol d'identité en ligne.

Les études effectuées jusqu'à présent ne se sont attardées que sur les activités en ligne à risque, l'utilisation de dispositifs informatiques et l'absence de gardien comme les logiciels antivirus pour expliquer la victimisation au vol d'identité en ligne. Pour le moment, aucune étude ne semble ainsi s'être attardée sur **les aspects cognitifs ou sur**

les caractéristiques de la personnalité (telle que l'impulsivité) des victimes.

Références

[1] Centre antifraude du Canada. (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] A ne pas confondre toutefois avec la fraude d'identité, qui consiste davantage en l'usurpation d'identité de quelqu'un sans pour autant commettre un vol de son identité (usage trompeur de renseignements identificateurs d'une autre personne dans le but de commettre diverses fraudes). (Centre anti-fraude du Canada. (2018). *Vol d'identité et fraude à l'identité*).

[4] Centre anti-fraude du Canada. (2018). Vol d'identité et fraude à l'identité.

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

[6] Centre anti-fraude du Canada. (2019). Données non-publiées.

[7] Cornelius, D. R. (2016). Online identity theft victimzation: 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. et Turner. M. G. (2012). Examining risks and protective factors of on-line identity theft. *Deviant Behavior*, *33*(4), 308-323.

[10] Paek, S. Y. et 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. et 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.