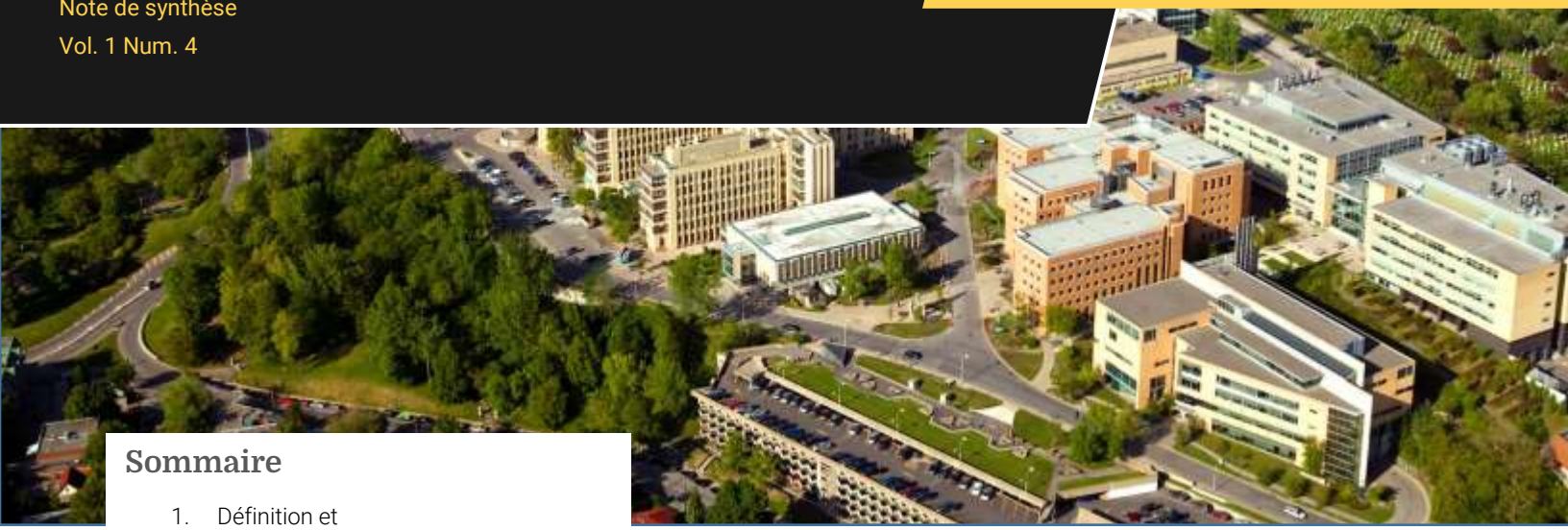
La fraude par marketing de masse

Morgane Coat, candidate à la maîtrise

Note de synthèse
Vol. 1 Num. 4

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

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

Définition et ampleur

La fraude par marketing de masse se définit comme « **tout acte faux, trompeur, fallacieux ou frauduleux visant à inciter les individus à envoyer de l'argent ou à fournir des renseignements personnels. Cela comprend les demandes ou offres non sollicitées reçues par téléphone, par la poste, par Internet, par courriel, ou encore au porte-à-porte** »[1]. Au Canada, en 2018, la fraude par marketing de masse a fait perdre près de **100 millions de dollars canadiens** aux victimes, dont **55 millions dans un contexte en ligne**[2].

Profil des victimes

- Généralement, il semblerait que **les hommes** soient davantage susceptibles d'être victimes de fraude[3] [4] [5].
- Les personnes âgées de **18 à 24 ans sont les plus susceptibles d'envoyer leurs renseignements personnels** en réponse à une invitation frauduleuse.
- Les personnes âgées de **65 ans et plus sont plus susceptibles d'envoyer de l'argent** que les autres groupes d'âge.
- Les personnes âgées de **35 à 44 ans sont celles qui sont les moins susceptibles** d'envoyer de l'argent à la suite d'une invitation frauduleuse[6].

Facteurs de risque

Il a été démontré que les victimes de fraude peuvent commettre plusieurs **erreurs de jugement motivationnelles et cognitives** dans leur prise de décision, parmi lesquelles[7 8 9 10] :

- Faire davantage confiance à ce qu'elles croient être des **personnes en position d'autorité**[10] ;
- Être plus sensibles aux **« déclencheurs viscéraux »** mis en avant par les fraudeurs[10]. Ces déclencheurs, tels que l'argent, le sexe, l'amour, la douleur et le chagrin, sont utilisés afin que les victimes potentielles se focalisent sur les avantages présentés par le fraudeur et qui sont liés à des états émotionnels futurs positifs imaginés;
- **Prendre des décisions plus rapides** face aux offres limitées dans le temps ou à la rareté de ces dernières;
- **Manquer de maitrise de soi**;
- Avoir un **excès de confiance en soi** et en sa capacité à détecter une éventuelle fraude parce qu'elles s'estiment davantage sensibilisées à cette problématique[7 10 11]. Cela s'explique par le fait que plus un individu a de connaissances dans un domaine spécifique, plus ils se sent compétent dans ce domaine et surestime donc sa capacité à prendre de bonnes décisions.
- Être à la recherche de **sensations fortes**.

Les victimes peuvent également être plus susceptibles de réagir à **certaines techniques employées par les fraudeurs**, tel que l'exercice de pressions ou de contraintes sur la victime, ou encore le fait de faire croire à cette dernière qu'ils partagent tous deux des centres d'intérêt communs[7 10].

Les victimes de cyberfraudes sont plus susceptibles d'**être impulsives** face à l'urgence ou face à la recherche de sensations fortes, d'être **dépendantes**, ou encore de s'engager davantage dans des **comportements risqués en ligne** tels que les achats sur des sites à l'étranger, les jeux en ligne, la participation à des forums de discussion et aux sites de rencontre, ainsi que les dépenses associées à la consommation de pornographie[12 13 14].

Certaines victimes effectuent souvent **plus d'efforts cognitifs** et passent plus de temps à analyser les fraudes que les non-victimes. Cela pourrait s'expliquer par le fait que les victimes ne savent pas forcément **comment identifier** les offres légitimes des offres frauduleuses [7 12 15].

Cette apparente contradiction avec le fait que les personnes impulsives sont également plus susceptibles d'être victimes de fraude s'expliquerait par le fait que certaines personnes impulsives peuvent à l'inverse supprimer directement une offre ou un courriel sans y accorder trop d'attention[7]. L'impulsivité influencerait ou non la susceptibilité d'être victime de fraude de deux manières différentes.

Les personnes ayant un **niveau de scolarité plus élevé**, celles qui pensent avoir **plus de contrôle sur les évènements externes** pouvant les affecter, et celles qui ont tendance à davantage faire preuve de **préméditation** sont également plus susceptibles d'être victimes de cyberfraude[12].

Les victimes de fraude ont tendance à **ne pas parler à leur entourage** des fraudes en cours ou de celles dont elles ont été victimes[16].

L'argent des victimes provient principalement de leurs **économies personnelles**. Toutefois, certaines vont jusqu'à contracter un prêt personnel, emprunter de l'argent à leurs proches ou hypothéquer des biens[9 17].

Certaines victimes ont beaucoup de **mal à croire** qu'il s'agit d'une fraude et peuvent **rester engagées** dans cette dernière, même après avoir été

prévenues par diverses autorités (police ou institutions financières)[9 16].

Entre **26% et 45% des victimes de cyberfraude seront à nouveau fraudées au moins une fois au cours de leur vie**. Toutefois, aucune véritable distinction ne semble exister entre les victimes uniques et les victimes répétées [9 18]. La différence entre ces deux types de victimes pourrait s'expliquer par des différences individuelles au niveau de leur influençabilité[7].

Diverses **théories ou constatations plus psychologiques** peuvent également expliquer les raisons pour lesquelles les victimes se font arnaquer[7 9], comme par exemple :

- **L'effet des coûts irrécupérables** (ou phénomène du quasi-gagnant) : les victimes qui ont déjà investi de l'argent dans l'arnaque une première fois, ou qui estiment avoir déjà beaucoup investi, pensent qu'en continuant à investir un peu plus, elles se rapprocheront de leur but et finiront par l'atteindre. Le phénomène du quasi-gagnant pourrait possiblement expliquer la dépendance aux arnaques et le fait que les individus aient du mal à s'en sortir.

- **Le pari risqué** : même si l'offre ne leur parait pas fiable, considérant les gains potentiels en jeu, les victimes sont incitées à tenter leur chance et pensent que cela en vaut la peine dans le cas où l'offre s'avèrerait finalement vraie.

Recommandations

L'**éducation** et la **sensibilisation** des individus est nécessaire pour que ceux-ci puissent apprendre à détecter les fraudes, ainsi que les différentes techniques de persuasion employées par les fraudeurs[16 19]. Ces campagnes doivent autant être généralistes, que ciblées selon l'âge des participants, leur mode de vie (activités à risque), ou les diverses technologies utilisées [6 7 20].

Les modèles prédictifs de la victimisation à la cybercriminalité, ainsi que toute approche visant à prévenir la victimisation aux fraudes, doivent tenir compte de **l'ensemble des caractéristiques des victimes** : leurs caractéristiques sociodémographiques et psychologiques, leurs traits de personnalité, leurs activités en ligne[12 20], ainsi que leurs divers processus motivationnels et cognitifs[7].

Étant donné que la connaissance d'une escroquerie peut ne pas être suffisante pour empêcher les individus de se faire frauder, il est nécessaire d'**élaborer des interventions autres que celles basées sur l'éducation ou la sensibilisation**, et d'aller au-delà du simple apprentissage de la détection d'une fraude [9 18].

Limites des études

Les études citées précédemment ne distinguaient pas forcément les fraudes en ligne des fraudes hors-ligne.

Considérant les nombreuses lacunes, contradictions ou incompréhensions quant aux résultats trouvés au sein des études, d'autres recherches sont nécessaires afin de mieux comprendre la victimisation aux fraudes.

Références

[1] (Traduction libre). 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] Centre anti-fraude du Canada. (2019). Données non-publiées.

[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 et 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. et 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. et 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. et 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. *The British Journal of Criminology*, *53*(4), 665–684.

[10] Button, M, Nichols McNaughton, C., Kerr, J. et 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. et 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. et 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, et 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. et 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. et Brown, K.(2015). "Winning and losing": vulnerability to mass marketing fraud. *Journal of Adult Protection*, *17*(6), 360-370.

[17] Ross, S. et Smith, R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice*, *420*(2011), 1-6, 1. Dans cette dernière étude, les chercheurs ont constaté que 80% de leurs participants avaient utilisé leurs économies personnelles pour répondre à la fraude, 13% d'entre eux avaient contracté un prêt, 10% avaient emprunté à leurs proches et 5% avaient hypothéqué des biens.

[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. et 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. et Dowell. D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology*, *34*(3)1-15.