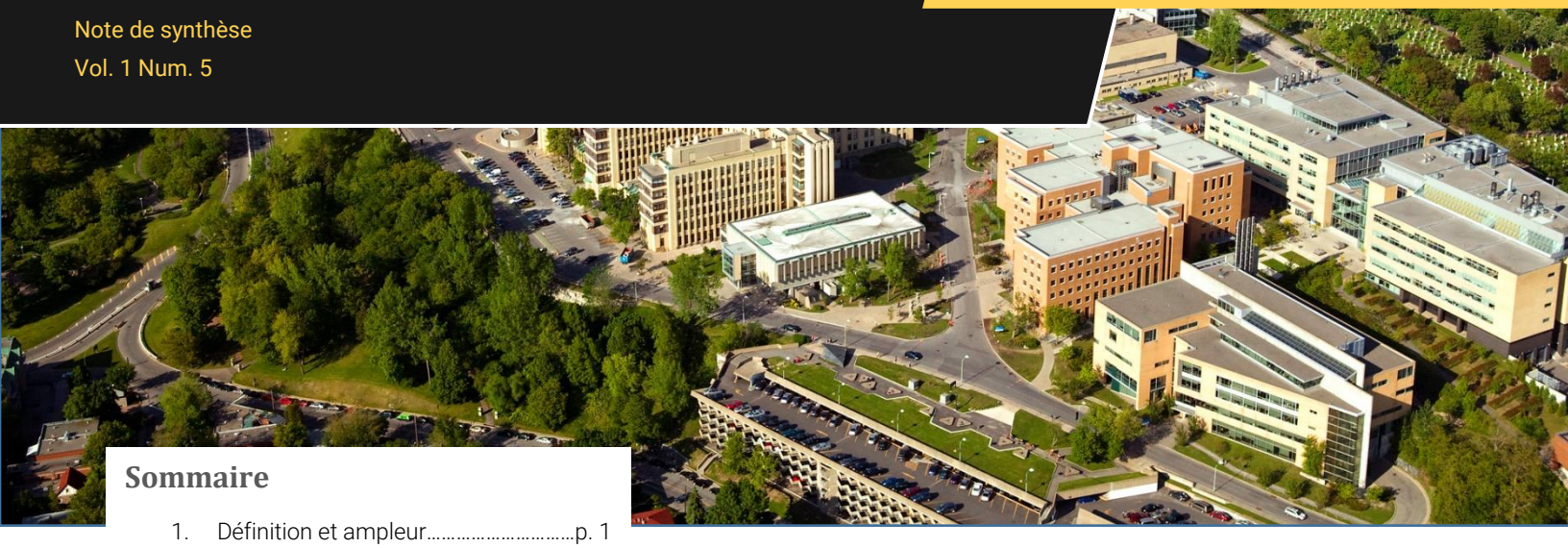
L'hameçonnage

Morgane Coat, candidate à la maîtrise

Note de synthèse
Vol. 1 Num. 5

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

L'hameçonnage correspond à : « tout courriel **prétendant provenir d'une organisation légitime** telle qu'une institution financière, une entreprise ou un organisme gouvernemental **dans le but d'inciter le destinataire à fournir des renseignements personnels et privés**. Le courriel peut demander au destinataire de visiter un site Web sur lequel on lui demande de mettre à jour ou de fournir des renseignements personnels ou financiers »[1]. Au Canada, en 2018, l'hameçonnage était **le type de fraude en ligne le plus signalé au Centre Antifraude du Canada**, avec **4417 signalements pour des pertes s'élevant à près de 100 000 dollars pour 1966 victimes**[2,3]. **Environ 1 personne sur 14** ayant été ciblée par un courriel d'hameçonnage clique sur le lien ou ouvre la pièce jointe contenue dans le courriel frauduleux[4].

Profil des victimes

La majorité des études les plus récentes avancent **que tous les individus, quel que soient leurs caractéristiques sociodémographiques** (sexe, âge, niveau d'éducation, ressources financières), **sont susceptibles d'être ciblés par un courriel d'hameçonnage, de cliquer sur le lien qu'il contient, et de fournir des renseignements personnels**[5,6,7,8,9]. Toutefois, **les femmes semblent avoir plus de difficultés à distinguer une page internet frauduleuse d'une page internet légitime** après avoir cliqué sur le lien contenu dans un courriel frauduleux[10].

Facteurs de risque et de protection

Les facteurs liés au fait d'être ciblé par une tentative d'hameçonnage

De nombreuses **activités routinières en ligne** (telles que, l'utilisation de services bancaires, les réservations, les achats et l'utilisation de réseaux sociaux) **augmentent les risques que les individus soient ciblés par des attaques d'hameçonnage**[11].

Il a également été démontré que les personnes ayant un comportement de « **copie numérique** », c'est-à-dire les individus qui ont largement recours à la copie, au partage et à l'utilisation de logiciels ou de contenus numériques, **augmentent leur risque de devenir des cibles d'hameçonnage**. Ces comportements n'étant pas toujours légaux, cela peut exposer davantage les individus aux cybercriminels[12].

De plus, **l'utilisation de dispositifs de système informatique** tels que les logiciels antivirus, les filtres de courriels, les systèmes de détection d'intrusion, **n'est pas pleinement efficace** pour empêcher les courriels d'hameçonnage de parvenir aux individus et ainsi, d'éviter leur victimisation[6 13].

Les facteurs liés au fait de cliquer sur le lien ou de répondre, ou non, à un courriel d'hameçonnage

Plus les individus ont de l'expérience et passent du temps sur internet, **moins ils sont susceptibles** de répondre à un courriel d'hameçonnage[14 15].

Autant pour les particuliers que pour les employés d'entreprises, les individus ont tendance à davantage cliquer sur un lien frauduleux **lorsque le courriel contient un message personnel ou provient d'une source connue**[8 16 17].

Au sein des entreprises, il a été démontré que les employés étaient **plus susceptibles de répondre à un courriel frauduleux** lorsque ce dernier contenait des **éléments d'urgence ou d'autorité**[15 16 17].

De plus, des facteurs contextuels en milieu de travail, tels que **le degré d'exposition aux courriels internes et externes**, l'utilisation de **boîtes de réception centralisées**, la **charge de travail**, la **surcharge d'informations dans l'environnement de travail**, ou **le rôle du soutien social et technique dans l'amélioration des perceptions d'auto-efficacité** (aide des pairs, bannières et interfaces d'aide) ont également été mentionnés comme ayant une **influence sur la probabilité de cliquer ou non** sur un courriel d'hameçonnage[16 19 20].

L'habitude et la routine sont également susceptibles d'augmenter le risque d'être victime d'hameçonnage[16 19 21].

Les personnes qui **sous-estiment la probabilité des cyberattaques et leur propre vulnérabilité** aux attaques d'hameçonnage sont plus susceptibles de cliquer sur un courriel frauduleux[22]. Deux études démontrent également qu'au sein d'un même pays, **les ressortissants étrangers détectent moins bien les indices au sein des courriels frauduleux** que les ressortissants de ce même pays[9 23].

Les facteurs liés à la détection, ou non, de pages internet frauduleuses résultant d'un courriel d'hameçonnage

Il a été démontré que les individus, même les plus expérimentés, **ont plus de difficultés à détecte**r les pages web frauduleuses lorsque ces dernières contiennent des **fenêtres pop-up ou des images et icônes en tout genre** (graphiques animés, images ou (faux) logos d'indicateurs de sécurité copiés sur Google)[10 24].

Certains **individus n'accordent pas beaucoup d'importance ou négligent les indices clés** comme la barre d'adresse, la barre d'état ou les indicateurs de sécurité. De plus, **certains individus ne font pas**

nécessairement confiance aux indicateurs de sécurité tel que le SSL, ou lorsque le nom de domaine ne correspond pas au nom de marque en raison de l'hébergement de pages web sécurisées auprès de tiers[10 24].

Les personnes qui passent plus de temps à inspecter une page ne vont pas forcément mieux détecter si cette dernière est frauduleuse ou non. Il existe un effet d'ancrage quant à la détection de pages web frauduleuses, c'est-à-dire qu'en raison d'un biais cognitif, la personne se fie fortement à la première information qu'elle reçoit. Passer plus de temps à inspecter une page aura donc moins d'efficacité dans la détection de pages frauduleuses[10 24].

Recommandations

Les formations et campagnes de sensibilisation à l'égard du grand public devraient être poursuivies de plusieurs manières différentes[8 9 13 15 17 22] :

- Mois de la sensibilisation à la fraude;
- Sensibilisation du public par les médias;
- Avertissements et conseils fournis par les institutions financières sur leur site internet;
- Exercice de simulation afin de reconnaître les pages web ou courriels frauduleux.

Ces mêmes campagnes et formations devraient s'attarder davantage sur divers points[7 12 24 18 19] :

- Les comportements qui rendent les utilisateurs vulnérables à l'hameçonnage et les comportements de protection à adopter pour l'éviter;
- Les limites des outils technologiques de protection;
- Les conséquences concrètes d'une attaque d'hameçonnage;
- Les différents indices pour reconnaître des courriels ou des pages web frauduleux et les distinguer des légitimes.

Au sein des entreprises, il est recommandé de tenir compte du contexte de travail des employés, et plus particulièrement de leur routine, habitudes et charge de travail, ou encore du nombre de courriels que ces derniers reçoivent. De plus, l'utilisation d'outils d'aide à la prise de décision, tels que des avertissements, bannières ou mises à jour des employés sur les menaces peuvent constituer une aide précieuse pour ces derniers. La vérification auprès des pairs est également conseillée en cas de doute d'un employé. Suite au signalement d'un courriel par un employé, il est également recommandé de fournir une rétroaction à ce dernier quant à son jugement par rapport au courriel signalé et afin qu'il ne considère pas son signalement comme une perte de temps[19 20].

Limites des études

Parmi les études, il n'existe pas de consensus quant aux individus qui doivent être considérés ou non comme des victimes d'hameçonnage (il s'agit soit des personnes ayant seulement reçu un courriel frauduleux, soit celles ayant cliqué sur un lien, soit celles ayant subi des pertes financières ou encore, celles ayant fourni des renseignements personnels).

Les statistiques officielles sous-estiment les cas d'hameçonnage car ce dernier est souvent signalé dans d'autres catégories comme le vol d'identité ou le piratage, qui peuvent être des conséquences de cette fraude[26]. De plus, beaucoup de victimes ne se rendent jamais compte qu'elles ont été fraudées[27].

La majorité des chercheurs ayant étudié l'hameçonnage ont constitué leur cadre théorique autour de la théorie des activités routinières de Cohen et Felson, selon laquelle les infractions se produisent entre un délinquant motivé et une cible

appropriée en l'absence de gardiens compétents[28]. Très peu d'autres théories explicatives de l'hameçonnage ont été explorées pour le moment.

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] Centre antifraude du Canada (2019). Données non publiées.

[3] Alors que le simple hameçonnage consiste en une attaque de grande ampleur ne ciblant aucun groupe en particulier (voir, Leukfeldt, E. R.(2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *International Journal of Advanced Studies in Computer Science and Engineering*, *4*(5), 1-7), il en existe également une variante, appelée « harponnage » (*spear-phishing*), qui consiste en un courriel d'hameçonnage ciblant plus spécifiquement certaines personnes ou certains groupes, à propos desquels le fraudeur aura effectué quelques recherches au préalable (Voir, Chaudhry, J.A, Chaudhry, S.A et Rittenhouse, R.G.(2016). Phishing attacks and defenses. International *Journal of Security and Its Applications*, *10*(1), 247-256). En 2018, au Canada, 197 signalements d'harponnage ont été effectués auprès du CAFC pour des pertes s'élevant à plus de 523 000 dollars (pour 116 victimes).

[4] Verizon Business RISK Team (2017). 2017 Data breach investigations report. 10th edition. Verizon Business.

[5] Les études expliquent ces résultats par le fait que les fraudeurs semblent effectuer des attaques de grande ampleur auprès de la population générale, sans chercher à cibler des populations particulières.

[6] Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555.

[7] 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.

[8] Moody, G. D., Galletta, D. F. et Dunn, B. K. (2017). Which phish get caught? An exploratory study of individual susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564-584.

[9] Broadhurst, R., Skinner, K., Sifnotis, N, Matamoros,-Macias, B. et Ipsen, Y. (2018). Phishing and Cybercrime Risks in a University Student Community. *International Journal of Cybersecurity Intelligence and Cybercrime*, *2*(1), 4-23.

[10] Iuga, C., Nurse, J. R. C. et Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences*, *6*(8), 1-20.

[11] Reyns, B. W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime*, *22*(4), 396-411.

[12] De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L. et Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277-1287.

[13] Hutchings, A. et Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'Net'?. Current Issues in Criminal Justice, 20(3), 433-45.

[14] Horton, M. et Wimmer, H. (2017). Email phishing susceptibility in a public school setting: identifying at-risk educators. *International Journal of Cyber Society and Education*, *10*(1), 31-46.

[15] Wright, R. T. et Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273-303.

[16] Vishwanath, A., Herath, T., Chen, R. et Wang, J. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, *51*(3), 576-586.

[17] Gordon, W. J., Wright, A., Aiyagari, R. (2019). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *JAMA network open*, *2*(3), 1-9.

[18] Alseadoon, I. M. A.(2014). The impact of users' characteristics on their ability to detect phishing emails (Doctoral dissertation, Queensland University of Technology).

[19] Williams, E. J., Hinds, J. et Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13.

[20] Conway, D., Taib, R., Harris, M., Berkovsky, S., Yu, K et Chen, F. (2017). A qualitative investigation of bank employee experiences of information security and phishing. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS}*, Santa Clara, CA, 115-129.

[21] Vishwanath, A., Harrison, B. et Ng, Y. J. (2015). Suspicion, cognition, automaticity model (SCAM) of phishing susceptibility. *Communication Research*. doi: 10.1177/0093650215627483.

[22] Halevi, T., Memon, N. et Nov. O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015).

[23] Butavicius, M., Parsons, K., Pattinson, M., McCormac, A., Calic, D. et Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. In *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017)*, 1-12.

[24] Dhamija, R., Tygar, J. D. et Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 581-590.

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

[26] Australian Competition and Consumer Commission (ACCC). (2019). Targeting Scams: Report of the ACCC on Scams Activity 2018.

[27] MacGibbon, A. (2005). *Australian e-Commerce Safety Guide 2005*.

[28] Cohen, L. E. et Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *4*, 588-608