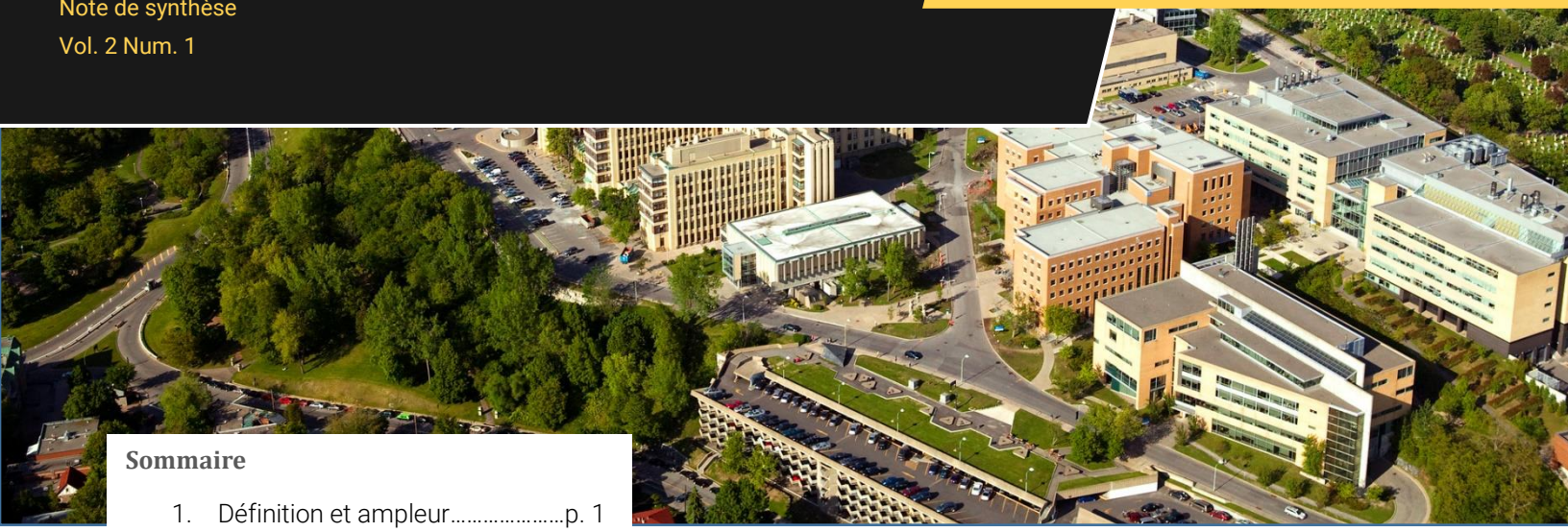
La fraude au soutien technique

Claire Gagnon, candidate à la maîtrise

Note de synthèse
Vol. 2 Num. 1

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

Bien que les définitions de la fraude au soutien technique soient nombreuses, il existe un consensus quant à ses principales caractéristiques. Ce type de fraude a lieu lorsque **des personnes se font passer pour des employés d'un centre de soutien technique et soutirent de l'argent à des individus en les persuadant qu'un virus ou un pirate informatique s'attaque à leur matériel technologique**[1].

Apparue il y a un peu plus d'une dizaine d'années[2], la fraude au soutien technique a évolué et s'est diversifiée. En 2018, **plus de six personnes sur dix** ont rapporté avoir été confrontées à une tentative de fraude au soutien technique[3]. Les données de l'année précédente estimaient que **3 millions d'individus par mois** étaient confrontés à cette menace[4]. Touchant majoritairement les particuliers, ce type de fraude est annuellement responsable d'importantes pertes financières. Avec une augmentation de 86% par rapport à 2016, les États-Unis rapportaient en 2017 des pertes s'élevant à 15 millions de dollars américains[5].

Fonctionnement

Trois quarts de ces organisations frauduleuses, dont le fonctionnement est similaire aux centres d'appels légitimes, sont basés en Inde. Les autres organisations sont localisées aux États-Unis et au Costa Rica. Elles se composent en moyenne d'une douzaine de faux techniciens[6]. Toutes ces organisations opèrent de manière similaire :

- La prise de contact initiale avec les potentielles victimes se fait de plusieurs façons :
  - Un appel ou courriel non sollicité;
  - La création d'une page internet conçue pour imiter les sites légitimes de soutien technique[4, 7]. Dans ce dernier cas, les fraudeurs utilisent des techniques de recensement non autorisées par les moteurs de recherches[7] afin de piéger l'algorithme de classification des moteurs de recherche pour que ceux-ci offrent aux sites qui les utilisent davantage de visibilité dans les résultats de recherche des consommateurs[8]. Les techniques peuvent impliquer une répétition ou utilisation excessive de mots-clés, parfois cachés sur les pages du site et sans liens avec le contenu[8].
  - La technique « TechBrolo », la prise de contact virtuelle la plus utilisée par les fraudeurs, est présente dans près de 61% des cas[4]. Celle-ci consiste en l'affichage d'un message alarmant depuis un site malveillant et dont il est impossible de se débarrasser sans fermer le navigateur via le gestionnaire de tâche.
- Si la prise de contact se fait par une autre voie que téléphonique, le fraudeur va chercher à établir un contact téléphonique avec la victime. Il se présente généralement comme employé d'un centre de soutien technique d'une grande entreprise technologique telle qu'Apple, Bell ou Microsoft. L'appel dure en moyenne 17 minutes[6].
- Le fraudeur va ensuite tenter de convaincre le consommateur de le laisser accéder à distance à l'appareil en question. Cet accès permet d'installer des logiciels espions ou de voler des données personnelles.
- Par la suite, le fraudeur identifie de fausses menaces sur l'appareil de la victime dans le but de lui facturer les services de soutien technique. Les fraudeurs font généralement preuve de patience et de créativité dans leurs techniques de persuasion[6]. Il est à noter que dans les cas où la victime est déjà convaincue qu'il y a un problème, l'accès à distance de l'ordinateur et l'utilisation de techniques trompeuses deviennent des étapes facultatives[2].
- La fraude est complète lorsque les fraudeurs reçoivent l'argent de la victime. L'utilisation de la carte de crédit comme paiement offre une certaine protection aux consommateurs qui dans la majorité des cas, récupèrent la totalité ou une partie de leur argent[9]. En 2018, **les paiements par cartes rechargeables et cartes cadeaux étaient de plus en plus demandés par les fraudeurs**[9], ce qui rend plus difficile, voire impossible, de retracer l'argent versé.
- La victimisation peut s'arrêter après le paiement ou continuer. En effets, certaines victimes deviennent des cibles spécifiques : tant qu'elles paient, elles sont sollicitées[5].
- Dans d'autres cas, les fraudeurs réalisent des fraudes complémentaires afin d'obtenir davantage d'argent[5]. Par exemple, certains se font passer pour des agents du gouvernement ou des policiers ayant pour but d'aider les victimes à recouvrer leur argent suite à la fraude au soutien technique. Le fraudeur

demande à la victime de payer des frais pour les démarches d'assistance ou de demande de remboursement[5]. D'autres cas se révèlent plus agressifs, telle la fraude consistant à prendre le contrôle de l'ordinateur ou d'un compte de la victime puis de lui demander une rançon. Dans d'autres cas, le fraudeur se fait passer pour un service de recouvrement et menace les consommateurs d'intenter une action légale contre eux s'ils ne paient pas pour les faux services de soutien technique rendus.

Profil des victimes

En 2018, sur l'ensemble des individus touché par cette fraude, **6% y ont perdu de l'argent**[3]. En 2016, ce pourcentage s'élevait à 9%. **Les pertes individuelles sont variables et oscillent généralement de quelques dizaines à quelques centaines de dollars**[6]. Dans des cas extrêmes, le montant peut s'élever à plusieurs dizaines de milliers de dollars[10]. Les conséquences dépassent souvent le simple cadre financier. En effet, plusieurs individus rapportent avoir perdu du temps à chercher ailleurs une solution au problème, et près de **trois individus sur quatre rapportent avoir vécu un stress moyen à sévère** après la tentative de fraude[3].

Bien que **les pays anglophones soient habituellement les plus ciblés par ce type de fraude[2], plus de 180 pays dans le monde ont été touchés**[3, 5, 10]. Les plaintes sont principalement émises par des consommateurs américains, canadiens, britanniques et européens[11]. Plus précisément, la majorité des tentatives de fraude via la technique du TechBrolo a eu lieu aux États-Unis où le pourcentage s'élève à 58% du total des cas recensés, soit près de 5 fois plus qu'au Royaume-Uni, second pays le plus touché (13%)[4]. Le Canada totaliserait quant à lui 11% du total des tentatives, suivi par l'Australie (8%), la France (4%) et l'Espagne (3%)[4].

La perte d'argent était moins importante en 2018 qu'en 2016 pour la majorité des pays, bien qu'il y ait eu une augmentation dans les pays qui en avaient auparavant le moins. Il est cependant important de prendre en compte la singularité de chaque pays[3]. Par exemple, l'Allemagne est le seul pays à signaler être majoritairement contactée par appel non sollicité[12]. Également, l'Inde rapporte le plus haut taux de victimes ayant perdu de l'argent dans cette fraude puisque celui-ci s'élève à 14% du total des tentatives, comparativement à un taux maximum de 9% pour les autres pays[3].

En 2018, Microsoft rapportait une moyenne de **11 000 plaintes par mois** pour des cas de fraude au soutien technique[13]. **Le nombre réel de victimes serait cependant largement sous-estimé** compte tenu du fait que certains individus ne se rendraient pas compte qu'ils ont été victimes de fraude[14]. Cela serait particulièrement le cas pour les consommateurs à l'initiative de l'interaction.

De plus, la fraude semble toucher différemment les individus en fonction de leur âge. **Les individus de plus de 54 ans semblent être plus touchés** par les appels non sollicités tandis que les individus plus jeunes consultent davantage les sites frauduleux[3].

Facteurs de risque et de protection

Considérant la diversification des points d'accès utilisés par les fraudeurs, **tous les individus utilisant un ordinateur peuvent devenir la cible d'une fraude au soutien technique**[14]. Quelques observations ont cependant été faites :

- D'après le sondage international et autorapporté de Microsoft en 2018, **les individus ayant entre 18 et 37 ans (9%) sont plus susceptibles de continuer l'interaction après la prise de contact initiale et sont plus nombreux à perdre de l'argent comparativement aux individus plus âgés (2%)**[3]. Une autre étude portant sur des données officielles des États-Unis observe cependant un phénomène inverse et rapporte que les individus plus âgés sont près de 4 fois plus à risque de perdre de l'argent dans ce type de fraude[9].

- Le genre de l'individu semble également montrer des différences au niveau de la victimisation. En effet, **les femmes (5%) sont moins susceptibles de perdre de l'argent comparativement aux hommes (7%)**[3]. Ces derniers sont également légèrement plus exposés à ce type de fraude. Malgré cette différence observable, une étude sur les victimes de fraude au soutien technique suggère que seul le fait d'être âgé de plus de 65 ans prédit une perte financière, tandis que le genre ou les revenus ne le permettent pas[15].

- **Être de la génération Z ou millénariale** est lié à plusieurs facteurs pouvant augmenter les risques pour l'individu d'interagir avec les fraudeurs et de perdre de l'argent[3]. D'après Microsoft, ces individus s'engagent davantage que leurs aînés dans des comportements en ligne à risque, comme par exemple partager leur compte courriel ou aller sur des sites de téléchargement[3].

- Considérant que les fraudeurs misent sur le manque de connaissance informatique des victimes, **les individus possédant de fortes connaissances ou étant employés dans le secteur du soutien technique sont moins susceptibles** de se laisser tromper.

- **Les individus activement à la recherche de soutien technique** sont plus à risque de naviguer sur des pages frauduleuses imitant celles qui sont légitimes[7]. À travers l'utilisation de diverses techniques de recensement non autorisées par les hébergeurs de site web ainsi que par l'achat d'emplacement de publicité dans les moteurs de recherche, ces sites réussissent à apparaître parmi les premiers résultats de recherche[7]. Dans ce cas, c'est le consommateur qui initie le contact et la fraude est donc moins facile à détecter.

- **L'éducation de la population constitue le meilleur rempart contre ce type de fraude**. Ainsi, lorsque le consommateur est conscient que les compagnies légitimes n'appellent pas directement leurs clients, cela lui permet d'être méfiant vis-à-vis des appels non sollicités d'un supposé centre de soutien technique[3]. De la même manière, les individus conscients que les sites web affichant un message alarmant et indiquant un numéro d'appel peuvent représenter une fraude seraient moins à risque de prendre contact avec les fraudeurs. Avoir été victimisé par ce type de fraude peut amener à plus grande méfiance, mais dans le cas où la victime de cette fraude n'a pas pris conscience de celle-ci, elle devient à risque de victimisation multiple. En effet, les fraudeurs s'échangent des informations sur les consommateurs qu'ils contactent et notamment sur ceux qu'ils réussissent à frauder, dans le but de leur soutirer davantage d'argent[5].

Recommandations

Bien que le nombre de plaintes pour fraude au soutien technique augmente, le nombre de personnes exposées à ce type de fraude ou y perdant de l'argent diminue[3]. Il s'agit d'une évolution encourageante faisant suite à plusieurs types de prévention.

Prévention sociale

La prévention auprès des consommateurs est le moyen le plus direct de contrer cette fraude. Sans nécessairement connaître le fonctionnement de la fraude, il est essentiel de savoir comment agirait un représentant légitime d'une compagnie. Les utilisateurs semblent davantage conscients de l'existence de ce type de fraude. En effet, **83% des individus sondés par Microsoft en 2018 affirment se méfier des appels non sollicités contre seulement 66% en 2016**[3]. Cela peut s'expliquer par le nombre croissant d'individus touchés à travers le monde et la dénonciation à travers les médias et réseaux sociaux.

Les campagnes de prévention telles que le mois de la prévention de la fraude au Canada sont également utiles afin de sensibiliser la population

aux différents types de fraudes. Ces campagnes encouragent les utilisateurs à détecter, contrer et signaler les fraudes. Le signalement de ces fraudes permettrait d'avoir une meilleure vision d'ensemble sur leur fonctionnement et leur évolution ainsi que de disposer de données plus fiables et utiles aux unités d'enquête et à des fins de recherches.

Considérant les singularités de chaque pays, la prévention doit être ciblée selon les pays. D'ailleurs, un rapport de Sécurité publique Canada sur la prévention de la fraude par marketing de masse apporte également des pistes d'actions intéressantes concernant la fraude au soutien technique. Ce rapport incite les pays à confronter leurs stratégies de lutte et à s'accorder sur les mesures à prendre contre les nouvelles manifestations de la fraude[16].

Plusieurs actions contre la fraude au soutien technique ont été menées conjointement par les forces de police, les gouvernements et des entreprises[17]. **Plusieurs organisations frauduleuses ont ainsi pu être démantelées** ces dernières années, comme peut en témoigner l'opération Tech Trap[16]. Cette opération illustre l'importance de collaborer au niveau international lorsque le délit est lui-même international.

Prévention technologique

À ce niveau, une collaboration entre les organismes privés, la police et le gouvernement est nécessaire. Plusieurs sont déjà en cours[15, 19, 20].

Contrairement aux pages web légitimes, **les pages hébergées par les fraudeurs apparaissent et disparaissent après un très court laps de temps**. En effet, la durée de vie moyenne d'une URL frauduleuse est de 11 jours[6]. Cette manœuvre permet d'éviter d'être mis sur la liste noire des moteurs de recherche, ou d'être supprimé par les forces policières[21]. Il est donc important de détecter ces pages le plus rapidement possible, car généralement, la détection par le public prend plusieurs semaines à quelques mois.

Afin de répondre à ce problème, quelques outils technologiques ont été créés. Par exemple, Notos est un outil technologique dynamique capable d'assigner un score de réputation à chaque nouvelle page web créée et permet ainsi de détecter les pages frauduleuses[21]. **Notos est capable de détecter quasiment 96,8% des pages frauduleuses et génère seulement 0,38% de faux positifs**. Un autre outil, spécifique aux fraudes au soutien technique, est ROBOVIC. Il se base sur les caractéristiques des publicités frauduleuses et permet d'automatiser leur découverte[6]. En somme, ces outils de détection peuvent servir à limiter l'exposition des consommateurs à ce type de fraude. À ce sujet, Microsoft affirme avoir rejeté 25 millions de publicités de fraude au soutien technique en 2017[22]. Ce nombre serait 5 fois supérieur à celui trouvé en 2016.

Considérant l'utilisation de techniques de recensement non autorisées par les moteurs de recherches7, une meilleure détection permettrait de repérer ces sites plus efficacement. Les sites de redirection, courants dans la fraude au soutien technique, ont une durée de vie plus longue que les sites hébergeant le contenu frauduleux7. L'objectif est alors de concentrer dans ces sites les techniques de référencement non autorisées afin qu'ils atteignent les victimes et les redirigent vers des sites au contenu

La littérature

Une définition commune et capable de prendre en compte les nouvelles formes de ce type de fraude est nécessaire. En effet, les études qui se rapportent aux fraudes au soutien technique peuvent parfois s'orienter vers un aspect précis et ainsi en omettre d'autres, tout aussi importants. Par exemple, la définition du Centre Anti-Fraude du Canada précise que la prise de contact s'effectue soit par un appel non sollicité, soit par une fenêtre publicitaire sur internet alors qu'il existe de nombreuses autres façons de prendre contact avec les potentielles victimes.

Il existe peu d'études sur le sujet et celles sur le profil des victimes sont également en nombre

limité. Il serait cependant pertinent, dans une optique de prévention, d'étudier plus en profondeur quels sont les facteurs de risque pour les victimes et notamment les risques de victimisation multiple. Les individus victimisés à plusieurs reprises peuvent devenir des cibles spécifiques des fraudeurs et perdre de plus grosses sommes d'argent. De plus, le fonctionnement interne des organisations criminelles reste absent de la littérature scientifique. Une meilleure compréhension de leur fonctionnement contribuerait à une meilleure efficacité des initiatives de prévention.

Références

[1] Centre antifraude du Canada. (2020, janvier 31). Service. Gouvernement du Canada. https://antifraudcentre-centreantifraude.ca/scams-fraudes/service-fra.htm#a7

[2] Rauti, S., & Leppanen, V. (2017). "You have a Potential Hacker's Infection" : A Study on Technical Support Scams. 2017 IEEE International Conference on Computer and Information Technology (CIT), 197-203. https://doi.org/10.1109/CIT.2017.32

[3] Microsoft. (2018). Global Tech Support Scam Research. https://news.microsoft.com/uploads/prod/sites/358/2018/10/Global-Results-Tech-Support-Scam-Research-2018.pdf

[4] Microsoft Defender ATP Research Team. (2017, avril 3). Tech support scams persist with increasingly crafty techniques. Microsoft Security. https://www.microsoft.com/security/blog/2017/04/03/tech-support-scams-persist-with-increasingly-crafty-techniques/

[5] Federal Bureau of Investigation (FBI). (2018, mars 28). Public Service Announcement. https://www.ic3.gov/media/2018/180328.aspx [6] Rickard Straus, R. (2020, 26 février). Fake job offer scam dupes thousands into laundering money for criminal gangs. *This is Money*.

[6] Miramirkhani, N., Starov, O., & Nikiforakis, N. (2017, février 27). Dial One for Scam : A Large-Scale Analysis of Technical Support Scams. Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2017.23163

[7] Srinivasan, B., Kountouras, A., Miramirkhani, N., Alam, M., Nikiforakis, N., Antonakakis, M., & Ahamad, M. (2018). Exposing Search and Advertisement Abuse Tactics and Infrastructure of Technical Support Scammers. WWW 2018: The 2018 Web Conference, 319-328. https://doi.org/10.1145/3178876.3186098

[8] Sharma, M., Khanna, Dr. A., & Sharma, P. (2017). Detection and Elimination of Search Engine Spam Using Various Techniques. International Journal of Pure and Applied Mathematics, 117(20). https://acadpubl.eu/jsi/2017-117-20-22/articles/20/90.pdf = 8

[9] Simons, J. J., Phillips, N. J., Chopra, R., Slaughter, R. K., & Wilson, C. S. (2019). Protecting Older Consumers 2018-2019 : A Report of the Federal Trade Commission. Federal Trade Commission. https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2018-2019-report-federal-trade-commission/p144401_protecting_older_consumers_2019_1.pdf =9

[10] Microsoft Defender ATP Research Team. (2018, avril 20). Teaming up in the war on tech support scams. Microsoft Security. https://www.microsoft.com/security/blog/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/ 10

[11] Gregoire, C. (2017, mai 18). The fight against tech support scams. Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2017/05/18/fight-tech-support-scams/ 11

[12] Chansanchai, A. (2018, octobre 15). Online scammers cost time and money. Here's how to fight back | Microsoft On The Issues. On the Issues. https://news.microsoft.com/on-the-issues/2018/10/15/online-scammers-cost-time-and-money-heres-how-to-fight-back/ 12

[13] Linn, A. (2017, juin 15). How Microsoft used AI to help crack down on tech support scams worldwide. The AI Blog. https://blogs.microsoft.com/ai/microsoft-used-ai-help-crack-tech-support-scams-worldwide/ 14

[14] Better Business Bureau (BBB). (2017). Pop-Ups and Impostors : A Better Business Bureau Study of the Growing Worldwide Problem of Computer Tech Support Scams. https://www.bbb.org/globalassets/article-library/tech-scam-study/bbb-computer-tech-support-study.pdf 13

[15] Jorna, P. (2016, novembre). The relationship between age and consumer fraud victimisation. Trends & Issues in Crime and Criminal Justice No. 519. https://www.aic.gov.au/publications/tandi/tandi519 15

[16] Federal Trade Commission. (2017). Operation Tech Trap : Law Enforcement Actions. https://www.ftc.gov/system/files/attachments/press-releases/ftc-federal-state-international-partners-announce-major-crackdown-tech-support-scams/operation_tech_trap_chart_of_actions.pdf 17

[17] Fair, L. (2017, mai 12). Operation Tech Trap targets tech support scams – and offers insights for business. Federal Trade Commission. https://www.ftc.gov/news-events/blogs/business-blog/2017/05/operation-tech-trap-targets-tech-support-scams-offers 16

[18] Sous-groupe de la fraude par marketing de masse, & Forum sur la criminalité transfrontalière. (2008). La fraude par marketing de masse. Rapport au ministre de la Sécurité publique du Canada et à l'Attorney General des États-Unis. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/archive-mss-mrktng-frd/archive-mss-mrktng-frd-fra.pdf 18

[19] Gregoire, C. (2018, novembre 29). New breakthroughs in combatting tech support scams. Microsoft on the Issues. https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/ 19

[20] Microsoft. (2018, octobre 18). Tech Support Scams are on the Decline but Canadians Still Need to be Vigilant. Microsoft News Center. https://news.microsoft.com/en-ca/2018/10/18/tech-support-scams-are-on-the-decline-but-canadians-still-need-to-be-vigilant/ 20

[21] Antonakakis, M., Perdisci, R., Dagon, D., Lee, W., & Feamster, N. (2010). Building a dynamic reputation system for DNS. Proceedings of the 19th USENIX Conference on Security. 21

[22] Kothari, S., & Garg, N. (2018, avril 17). Ad quality year in review 2017. Microsoft Advertising. https://about.ads.microsoft.com/en-us/blog/post/april-2018/ad-quality-year-in-review-2017 22