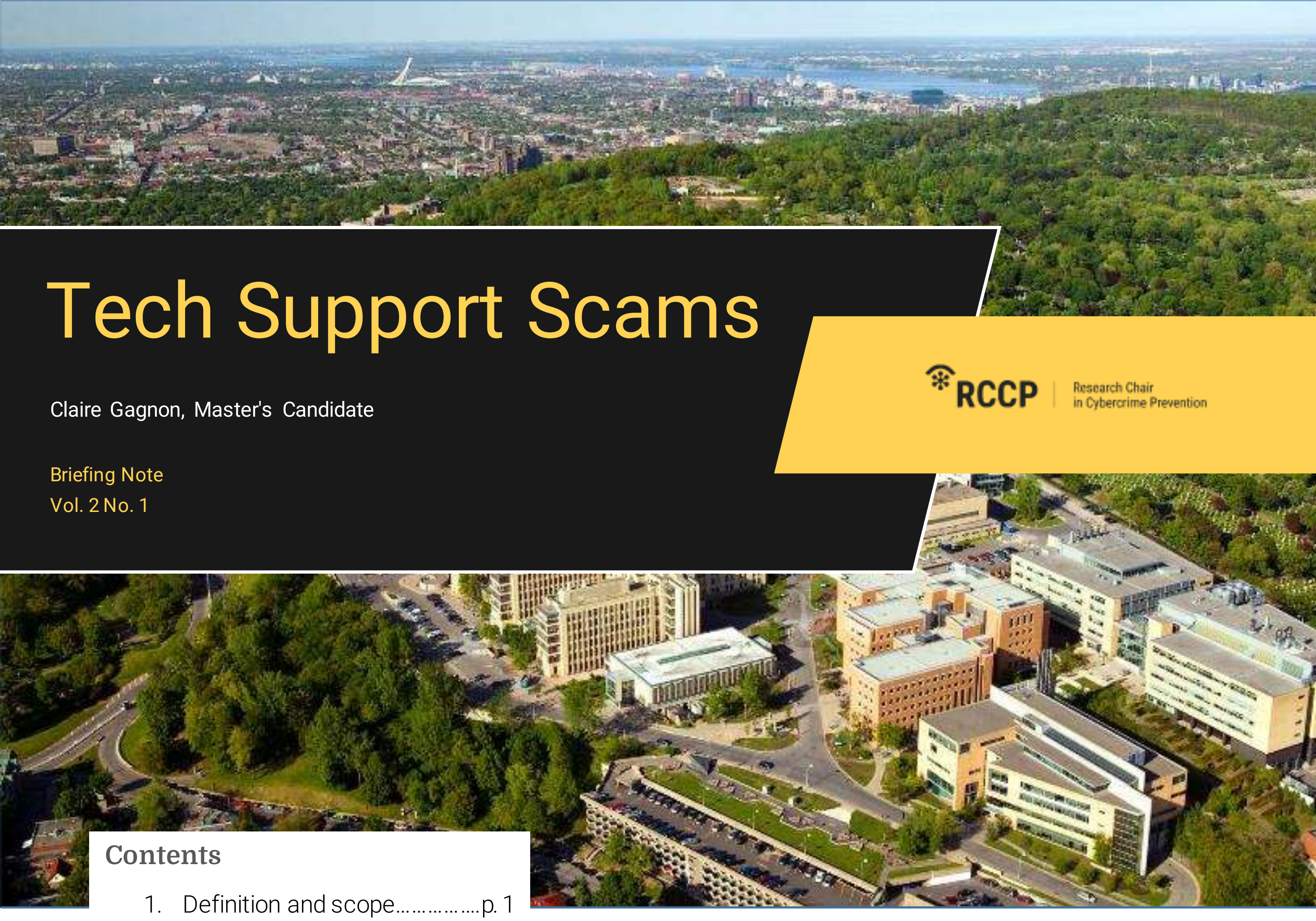

Tech Support Scams

Claire Gagnon, Master's Candidate

Briefing Note
Vol. 2 No. 1

RCCP | Research Chair in Cybercrime Prevention

Contents

1. Definition and scope……………p. 1
2. How the scam works…………..p. 1
3. Victim profile………………………p. 2
4. Risk and prevention factors……………………………………p. 3
5. Recommendations………………p. 4
6. References…………………………p. 5

Definition and scope

While there are many definitions of tech support scam, there is a consensus on the main characteristics. This type of scam occurs when **individuals impersonate technical support centre employees and steal money from people by persuading them that a virus or hacker is attacking their computer.**[1]

Emerging on the scene just over 10 years ago,[2] tech support scams have evolved and become more diverse. In 2018, **more than 6 out of 10 people** reported having experienced a tech support scam attempt.[3] According to data from the previous year, an estimated **3 million people per month** had encountered this threat.[4] This type of scam mainly affects individuals and is responsible for substantial financial losses every year. With tech support scams up 86% compared with 2016, the United States reported losses of US$15 million in 2017.[5]

How the scam works

Three-quarters of the organizations responsible for these scams, which operate similarly to legitimate call centres, are based in India. The rest are located in the United States and Costa Rica. They consist of 12 or so fake technicians on average.[6] All of these organizations have a similar operating method:

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

- Initial contact is made with potential victims in several ways:
  - An unsolicited phone call or email
  - A web page designed to resemble a legitimate technical support website is created.[4, 7] To do so, scammers use survey techniques not authorized by search engines[7] to trap the classification algorithms of search engines and give websites that use these search engines greater visibility in consumer search results.[8] The techniques can involve repetition or excessive use of keywords that may be hidden on website pages and not linked to the content.[8]
  - TechBrolo, the virtual contact technique most popular with scammers, is used in nearly 61% of cases.[4] It consists of displaying an alarming message from a malicious site that cannot be removed without closing the browser in Task Manager.
- If contact other than by phone is made, the scammer will try to establish phone contact with the victim. Usually, the scammer introduces themselves as an employee of a technical support centre of a major technology company, such as Apple, Bell or Microsoft. The call lasts an average of 17 minutes.[6]
- The scammer will then try to persuade the consumer to allow remote access to their device. Once allowed remote access, the scammer can install spyware or steal personal data.
- Then the scammer identifies false threats on the victim's device in order to bill the victim for technical support services. Scammers are generally patient and creative in the persuasion techniques they use.[6] It should be noted that in cases where the victim is already convinced there's a problem, remote access to the computer and the use of deceptive techniques become optional.[2]
- The scam is successful when the scammers receive money from the victim. Using a credit card for payment provides some protection for consumers, who recover all or a portion of their money in most cases.[9] In 2018, **scammers increasingly requested payments by reloadable cards and gift cards**.[9] This makes it more difficult, if not impossible, to trace the money paid.
- Victimization may stop after payment or may continue. In fact, some victims become specific targets: as long as they pay, they keep getting solicited.[5]

  In other cases, scammers engage in additional scams to obtain more money.[5] For example, some impersonate government officials or police officers trying to help victims recover their money after a tech support scam. The scammer asks the victim to pay a fee for assistance or reimbursement.[5] Other scams are more aggressive, such as taking control of the victim's computer or account and then demanding a ransom. In other cases, the scammer masquerades as a collection agency employee and threatens consumers with legal action if they don't pay for the bogus technical support services provided.

Victim profile

In 2018, **6% of all individuals affected by this scam lost money**.[3] In 2016, the percentage was 9%. **Individual losses vary and generally range from less than $100 to a few hundred dollars**.[6] In extreme cases, the amount can be in the tens of thousands of dollars.[10] The consequences are often more than financial: Many individuals report having wasted time looking elsewhere for a solution to the problem, and nearly **3 out of 4 report**

having felt moderately to severely stressed after the scam attempt.[3]

Although **English-speaking countries are usually the most targeted by this type of scam,**[2] **more than 180 countries around the world have been affected**.[3, 5, 10] The complaints are mainly from American, Canadian, British and European consumers.[11] More specifically, most scam attempts using the TechBrolo technique occurred in the United States, with 58% of the total number of cases recorded, nearly five times higher than in the United Kingdom, the second most affected country (13%).[4] Canada saw 11% of total attempts, followed by Australia (8%), France (4%) and Spain (3%).[4]

Most countries lost less money in 2018 than in 2016, although countries that had previously reported the lowest losses saw an increase in those losses. However, it is important to consider the uniqueness of each country.[3] For example, Germany is the only country to report that the majority of calls are unsolicited.[12] Also, India reports the highest rate of victims who lost money in this type of scam, precisely 14% of all attempts, compared to a maximum of 9% for other countries.[3]

In 2018, Microsoft reported an average of **11,000 complaints per month** about tech support scams.[13] **However, the actual number of victims is vastly underestimated**, given that some people fail to realize they are scam victims.[14] This is particularly true of consumers who initiate interaction with a scammer.

In addition, scams appear to affect people differently, depending on their age. **People over age 54 appear to be more affected** by unsolicited calls, while younger people are more likely to visit scam websites.[3]

Risk and prevention factors

Considering the variety of access points used by scammers, **all computer users can become the target of a tech support scam**.[14] However, a few observations have been made:

- According to Microsoft's international self-reported survey in 2018, **individuals between 18 and 37 (9%) are more likely to continue the interaction after initial contact. A greater number will lose money compared to older individuals (2%)**.[3] However, another study of official US data observed the opposite, reporting that older individuals are almost four times more at risk of losing money in this type of scam.[9]

- Victimization also appears to vary by gender. **Women (5%) are less likely to lose money than men (7%)**.[3] Men are also slightly more exposed to this type of scam. Despite this observable difference, a study of victims of tech support scams suggests that being over age 65 alone is a predictor of financial loss, while gender or income is not.[15]

- **Several factors can increase the risk of interacting with scammers and losing money for generation Z or millennial individuals**.[3] According to Microsoft, these individuals engage more than their elders in risky online behaviour, such as sharing their email account or visiting downloading sites.[3]

- Considering that scammers rely on victims' lack of computer knowledge, **individuals who are very knowledgeable or employed in the technical support sector are less likely** to be fooled.

- **Individuals actively seeking technical support** are more likely to browse scam websites imitating legitimate websites.[7] By using survey techniques not authorized by website hosts and purchasing advertising space in search engines, these websites manage to come up in initial search results.[7] In this case, the consumer initiates contact, and the scam is, therefore, less easily detected.

- **Public education is the best defence against tech support scams**. So when consumers know that legitimate companies don't call their customers directly, they will be suspicious of unsolicited calls from a so-called technical support centre.[3] Similarly, individuals who know that websites displaying an alarming message and a number to call might be a scam will be less likely to contact scammers. Being a victim of this type of scam may lead to greater mistrust, but if the victim fails to realize what had happened, they will be at risk of being scammed again. Scammers share information about the consumers they contact, including those they manage to scam, in order to steal more money from them.[5]

Recommendations

While the number of complaints about tech support scams is increasing, the number of people exposed to or losing money to this type of scam is decreasing.[3] This encouraging development is the result of several types of prevention.

Social prevention

Prevention through consumer awareness is the most direct way to combat tech support scams. Without knowing how a scam works, consumers need to know how a legitimate company representative would act. Users appear to be more aware of this type of scam. In fact, **83% of individuals surveyed by Microsoft in 2018 said they were wary of unsolicited calls, compared to only 66% in 2016.**[3] This can be explained by the increasing number of people affected worldwide and by reporting in the media and social networks.

Prevention campaigns, such as Fraud Prevention Month in Canada, are also helpful in raising public awareness of various types of fraud. These campaigns encourage users to detect, combat and report fraud. Reporting these scams would provide a better overview of how they work and evolve and more reliable and valuable data for investigative units and research purposes.

Given each country's unique characteristics, prevention must be targeted to each one. A Public Safety Canada report on the prevention of mass marketing fraud also provides interesting insights into tech support scams. The report encourages countries to look at their strategies for combating fraud and agree on what to do about new types of fraud.[16]

Several measures to combat tech support scams have been carried out jointly by police forces, governments and businesses.[17] Consequently, a **number of fraudulent organizations have been dismantled** in recent years, for example, through Operation Tech Trap.[16] This illustrates the importance of international cooperation when the crime itself is transnational.

Technological prevention

To prevent tech support scams, a collaboration between private organizations, police and government is necessary. A number of initiatives are already in progress.[15, 19, 20]

Unlike legitimate websites, **sites hosted by scammers appear and disappear quickly**. In fact, the average lifespan of a fraudulent URL is 11 days.[6] This prevents fraudulent sites from being blacklisted on search engines or deleted by police forces.[21] So it's important to detect these websites as quickly as possible because it usually takes several weeks or months for the public to detect them.

A few technology tools have been created to address this problem. For example, Notos can dynamically assign a reputation score to each new domain created, thus enabling the detection of malicious domains.[21] **Notos can identify malicious domains with almost 96.8% accuracy and a low false-positive rate (0.38%)**. Another tool for detecting tech support scams is ROBOVIC. It uses the characteristics of malicious advertising to perform automated detection.[6] Detection tools like these can be used to limit consumer exposure to this type of fraud. In that regard, Microsoft claims to have removed 25 million tech support scam ads in 2017.[22] This was five times the number found in 2016.

Knowing that fraudulent sites use survey techniques not authorized by search engines,[7] better detections would allow these sites to be identified more efficiently. Redirect sites, which are common in tech support scams, have a longer lifespan than sites hosting malicious fraudulent content.[7] Unauthorized search engine optimization techniques are then concentrated on these sites to reach victims and redirect them to content sites.

Literature

A standard definition is needed that includes new forms of tech support scams. Studies of such scams sometimes focus on one specific aspect and overlook others that are just as important. For example, the Canadian Anti-Fraud Centre definition specifies that contact is made either through an unsolicited call or through a website pop-up, whereas there are many other ways to contact potential victims.

There are few studies on the topic and limited research on victim profiles. However, with a view to prevention, it would be appropriate to carry out a more in-depth study of the risk factors for victims, particularly the risks of multiple scamming. Individuals who have been scammed repeatedly can become specific targets for scammers and lose more money. The scientific literature also contains no information on the internal workings of criminal organizations. A better understanding of how they work would contribute to more effective prevention initiatives.

References

[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