Can we ever stop technical support scams?

To many who are not well-versed with technology, a computer is like a magic box that might work or fail on a whim, and when it fails, it is impossible to fix. Unlike that in physical objects, software failures are virtual and cannot be examined like a car engine, and its intangibility gives a sense of powerlessness in the non-technical users. Technical support scammers, or tech scammers in short, make use of this opportunity to first convince users that their computers are faulty for whatever reason, before pretending to give technical help to the victims, but instead scams money from them. These scams incur a big sum of money in general, even in a country of relatively small population like Singapore ("S$7.7m stolen through ‘tech support’ scams in first four months of this year, up 45 times from last year", 2020).

With so much monetary loss, sometimes up to a few thousand USD per scam, we might ask, is there any way to stop technical support scams? With the whole world getting more familiar with technology, and technical help getting more accessible, can we ever eliminate tech support scams? I argue that it is almost impossible, due to the increasing complexity and closeness of computer software systems, the inefficiency of help systems in tech, as well as the how education and law enforcement fall short to combat such tech scammers.

First of all, technology is getting extremely complex in today’s world (Andersen, 2014), software systems have their source codes spanning millions of lines of codes (McCandless, 2015). For example, in 2015, Microsoft Office is already known to have 45 million lines of code, and Facebook at around 65 million lines. These systems, when used in our daily lives, are not only prone to error more than simple code (Tanenbaum, 2002), and when they error, it is difficult to pinpoint exactly what happened. To a layperson, if a simple click can lead to almost “magical” effects, so can an accidental click ruin the whole system. This erroneous belief made the users more likely to believe when a malicious website of aggressive pop-up message telling them they have accidentally destroyed the system, leading them to look for help immediately. The tech support scammers then can exploit this moment of vulnerability and carry out the scams on the pretext of helping the users resolve these vulnerabilities.

Furthermore, when a user faces a problem, the inefficient and frustrating process of technical support available makes them even more vulnerable to the promises made by tech scammers. For example, many people are familiar with the “Troubleshoot” button on many Microsoft Windows systems that often returns useless messages such as “There are no errors detected on the system”. Coupled with slow and inefficient phone calls dealing with technical issues that usually orders the user to do the routine procedures of restarting the application, clearing the cache, reinstalling the application, and rebooting the system, but did not solve any problem, scam calls often seem more “appealing” (Tabron, 2021). They usually start with instructing the victims installing softwares on their system that allow remote access, then they begin with a series of operations which might seem technical and professional to the normal user. With proactive attitude and seemingly resourceful operations, they seem more appealing and effective to normal troubleshooting methods, which lead to the proliferation of such scams.

Many would claim that by educating the public and raising public awareness about technical support scams, most scammers would be less likely to stand a chance. Although this is theoretically correct, we also have to take into account the psychological techniques used by the scammers (Tabron, 2021). It is easy to teach people that “do not trust calls from unknown numbers”, “check the reliability of the website before you trust its contents”, but in the current world, many things can be faked, including the legitimacy of a website and its perceived trustworthiness. Many scam websites are specifically designed to induce panic in its users, such as mimicking the “Blue Screen of Death” (BSOD) in Microsoft Windows, as well as using flashing colours and a countdown timer creating a sense of urgency (Miramirkhani, Starov & Nikiforakis, 2017). Many of them are highly indistinguishable from the authentic warnings, and thus many victims cannot make a correct judgement at the moment. Once the victims believe that these information are true and make the call to the scammers, it is a battle half lost. Scammers are known to use techniques that earn the trust of victims (“I am here to help”, “We will resolve your issues immediately”), build rapport (“You remind me of my grandmother”), implicitly blame the victims (“Was it you who used the computer before the error happen?”, “Did you do XXX action yourself?”), as well as cutting out external support (“Do not tell anyone about this, if not bad things will happen”). It is hard to recover the critical thinking abilities when one is subjected to these treatments when vulnerable, making the scams hard to ward off by just raising awareness.

In conclusion, the persistence of technical support scams despite attempts to cull it is a two-pronged one: the software systems themselves getting extremely complex and hard to troubleshoot, as well as scammers using increasingly sophisticated psychological techniques in their scams. Although it might be possible to slowly reduce these incidents as people learn from their experiences, it would be difficult to completely eliminate technical support scams.

## **References**

Andersen, R. (2014). Is technology making the world indecipherable? – Samuel Arbesman | Aeon Essays. Retrieved 7 April 2021, from https://aeon.co/essays/is-technology-making-the-world-indecipherable

Browning, J. (2019). *Inside a scam call center* [Video]. Retrieved from https://www.youtube.com/watch?v=xb\_rgQ4IDS8

McCandless, D. (2015). Million Lines of Code — Information is Beautiful. Retrieved 7 April 2021, from https://www.informationisbeautiful.net/visualizations/million-lines-of-code/

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2017). Dial One for Scam: A Large-Scale Analysis of Technical Support Scams. *Proceedings 2017 Network And Distributed System Security Symposium*. doi: 10.14722/ndss.2017.23163

S$7.7m stolen through ‘tech support’ scams in first four months of this year, up 45 times from last year. (2020). Retrieved 7 April 2021, from https://www.todayonline.com/singapore/s77m-stolen-through-tech-support-scams-first-four-months-year-45-times-last-year

Tabron, J. (2021). *Creating Urgency in Tech Support Scam Telephone Conversations* (Degree of Master of Arts). Hofstra University.

Tanenbaum, A. (2002). *Computer networks by Andrew S. Tanenbaum*. Prentice Hall.