

Cyber Scams and You: Prevention and Education

Senior Project

In partial fulfillment of the requirements for

The Esther G. Maynor Honors College

University of North Carolina at Pembroke

By

Joshua Clubb

Department of Mathematics and Computer Science

4/28/2023

Joshua Hayden Clubb 4/28/23

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Honors College Scholar Date

Dr. Prashanth BusiReddyGari, Ph.D

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Faculty Mentor Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Joshua Kalin Busman, Ph.D. Date

Senior Project Coordinator

Acknowledgements

I would like to thank my friends and family for helping me so much during my time making this project. I would also like to thank my mentor for his guidance along this entire experience.

Abstract

The rise of online scams has become a growing concern for internet users around the world. Data from the Federal Trade Commission's annual reports reveals a worrying pattern of rising fraud complaints and losses, in spite of the widespread notion that these schemes are simple to recognize. This essay tries to raise awareness of internet scammers by describing several sorts of scams, their tactics, and objectives, as well as the universal warning signs that most frauds display. The paper discusses and presents examples of different fraud types, ranging from those that require active manpower, like refund scams, and those that use software to take a more passive route, like phishing, and trojan viruses. The essay also covers the methods fraudsters use to identify potential victims and the characteristics of targets. In order to avoid falling for these frauds, it emphasizes the value of education and prevention in its conclusion.

Cyber Crimes and You: Prevention and Education

Theft has been a part of human nature since the beginning. People have and always will compete for resources, and some people decide the best way to get resources is to take them from others. Scammers try to do this without the victim even knowing it ever happened to begin with. They attempt to get people to trust them with their hard-earned money before running off with it, leaving the victim to wonder what happened. This practice has changed over the years, and now they have the process down to a science. Using the Internet, they flood the web with fake ads, websites, emails, and phone numbers, all of which lead victims directly to them. My goal with this project was to bring awareness to online scams with a poster detailing some types of scams, their goals and methods, and some common red flags that most of these scams often share.

Firstly, some people may initially think that online scammers are not a big deal. These people may think that it is easy to spot a scam and most reasonable people can spot it when they are talking to one. However, the data shows otherwise. Every year the Federal Trade Commission (FTC) reports the yearly total number of fraud complaints and total amount of money lost to fraud, and it shows a disturbing trend (Vedova, 2022). Figure 1 shows a table containing the data from each of the FTC’s reports, from 2006 to 2022. The data clearly shows that as more and more people become reliant on the internet, scammers too are taking advantage of the new tech, leading to more and more money being stolen every year. Not to mention that this is also only the reported amount, there are likely many cases of people getting scammed and still not even realizing it, leading it to go unreported. In 2022, we saw a staggering $8.8 billion lost to fraud, with 5.2 million complaints, an increase of 1313% and 518% respectively since the start of the data in 2006.

**Figure 1.**

*Federal Trade Commission Fraud and Loss Reports.*

In order to avoid joining the statistics, we must learn how the scammers work, their methods, and their goals. The first step scammers take is to decide what approach to take. There are many different types of online scams, all of which can be avoided with the proper education on how they work. First is Phishing, which is likely the easiest type of scam. Phishing is when a scammer sets up a fake website that tries to look exactly like a real website, for example, Facebook. These dummy sites also have a box for the user to enter their login information. Since the site looks exactly like Facebook, the victim puts in their Facebook information, but instead of getting logged in like normal, their information is harvested by the fake site and stored away. The main goal is for the victim to give up their login information, and once that is done they can try that username and password on other sites, send out more scams to the victim’s friends, and even try to change the password to ensure the owner stays locked out. All of these can be very detrimental to someone, especially if they manage to find payment info on the site they get access to.

Another type of scam is the Refund Scam. This one starts with a phone call to a victim, where the scammer tells a story about their service that the customer has previously paid for is now going to come to an end, but before they shut down their doors they want to send back all the money that was left on the user’s service period. It is important to know that the victim has not paid for this service ever, since this would be the first time they hear about it. However, the promise of free money is an enticing one, so the victim goes along with it. Eventually, the scammer asks for access to the victim’s computer using a remote access software like TeamViewer. Once they can use the victim’s PC, they log into their bank website and use inspect element on the balance page to show that the victim has received more money than they were supposed to, so now the victim has to send some back. The scam comes from the fact that the victim was never given any money at all, the website was just manipulated to make it look like they did. However, some people might not know that you can do this, so they will gladly send back the amount they were not supposed to get, when in reality they just sent their own money and got nothing in return.

The next step for any scam is to find potential victims. Scammers work together and share information with one another, some of that information includes valid email-addresses and phone numbers. Scammers will sell each other lists of hundreds of these contact methods and send out phony emails and calls to each of them. They keep track of which ones gather responses, who answers the calls, and more. Of course, this is not the only way they find victims. They also make fake ads and posts all over the internet. These ads and social media posts usually contain a phone number that leads to the scam HQ or a link to a fake website to harvest information. Since their fake websites usually have very strange web addresses, they often use a link-shortening service like bitly, so their link does not look suspicious at first glance.

In addition to the methods listed above, there is another way that scammers look for victims. Robocalls. A robocall is a call sent out by a computer or program with a prerecorded message with the intention of the call receiver getting transferred to an active scammer to get their money. These robocalls were a very big problem a few years ago, with many people getting these calls daily. Although they seem to have slowed down now, they are certainly still in use. These robocalls were usually easy to spot, leading to many people ignoring them, but some still got hooked. There were solutions to avoid these robocalls, including different apps that filtered them out and SnorCall, which allows the user to easily determine the content of a robocall, which can be used to determine what type of scam it is, how much money they are looking for, and who might be involved with it (Prasad et al.).

What makes someone a likely victim though? A survey and subsequent study with 11,534 participants found that individuals with weak self-control ability appear to be the primary targets of Internet scams, while online shopping and opening emails from unknown sources positively predicted being an Internet scam victim. The study suggests that individuals need to understand how Internet scams work and resist the desire for immediate monetary benefits to avoid becoming a victim (Chen et al., 2017, p. 9). This lack of self-control leads people to believe things they might otherwise be cautious about. Those with more self-control may think twice before clicking strange links that promise things too good to be true.

Once the scammers have a victim in their hands, their next steps depend on what type of scam they’re doing. There are several different approaches they like to use. If their scam involves direct contact, like the refund scam or others like it, then they will carry out the instructions that their script has, to mislead the victim and string them down a path which only leads to sending money to the scammer. The main method they use to accept money is through gift cards. They request that the victim drive to a nearby store and buy hundreds of dollars worth of gift cards to use as payment for whatever service the scammer claims to offer. The main reason they use gift cards is because it is untraceable. Once a gift card is purchased and then the code is sent, it becomes essentially impossible to get it back. Sometimes they will also accept Bitcoin as payment, since that is also hard to trace down and get back.

Some scammers do not want to get directly involved with their victims though. They instead would opt to use a software-based solution to getting money from their victims. This includes the phishing sites detailed earlier, but there is much more than that. One type of software they might make is a Trojan. A Trojan virus is a piece of software that claims to be one thing but is actually a virus that harvests your information or corrupts your files. This can happen due to negligence by the victim or by complete accident, and the easiest way to avoid them is to stick to using trusted websites and avoid clicking any suspicious links or downloads. Besides Trojans though, there are many other types of malware, like Keyloggers. A keylogger is a piece of software that runs in the background, out of sight of the victim, and secretly monitors every single keyboard stroke and mouse click. Advanced keyloggers can also filter out junk inputs from actual strings of words and intentional inputs. This information is sent to another computer, which can use the inputs to find login information, bank details, and more. The best way to avoid this is to again use trusted sites, but it also helps to have your passwords saved on sites you use, in order to avoid retyping them over and over.

However, there are ways your information can be stolen due to no fault of your own. Occasionally, a big company will experience a data breach. A data breach is when customer information is posted online publicly after a large database of information was compromised and stolen. This happens to a lot of companies, and there is nothing a single user can do to avoid it, as these data breaches usually consist of thousands or millions of user logins or payment info. The only thing a person can do to recover from one of these is to change their passwords on all of their accounts that use that email, or at least accounts that share that password. It is also worth noting that since these data breaches have such an excessive amount of user data, the likelihood of someone picking yours out at random would be very low, but not impossible.

In conclusion, online frauds are a significant problem in today's society and they are evolving rapidly. Scammers are taking advantage of the new technology and robbing more and more people of their money every year as more people rely on the internet for their everyday requirements. In order to avoid being a victim, it is critical for people to be informed of the many sorts of scams, their objectives, and their techniques. We can defend ourselves and our personal information against con artists who are always hunting for new victims by being knowledgeable and educated. Remember, prevention is vital, and we can all help lessen the impact of cybercrime by remaining watchful and careful.

References

Chen, H., Beaudoin, C. E., & 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. https://doi.org/10.1016/j.chb.2017.01.003

Iacurci, G. (2022, February 22). Consumers lost $5.8 billion to fraud last year - up 70% over 2020. CNBC. Retrieved February 22, 2023, from https://www.cnbc.com/2022/02/22/consumers-lost-5point8-billion-to-fraud-last-year-up-70percent-over-2020.html

Prasad, S., Dunlap, T., Ross, A., & Reaves, B. (n.d.). *Diving into robocall content with SnorCall*. USENIX. Retrieved April 27, 2023, from https://atc.usenix.org/conference/usenixsecurity23/presentation/prasad

Vedova, H., & Technology, T. F. T. C. O. of. (2022, March 5). Consumer Sentinel Network Reports. Federal Trade Commission. Retrieved April 8, 2023, from https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

*What are some common types of scams?* Consumer Financial Protection Bureau. (2022, October 17). Retrieved February 22, 2023, from https://www.consumerfinance.gov/ask-cfpb/what-are-some-common-types-of-scams-en-2092/