The Effect of Cyber Security Attacks on People’s Lives

Ulric Aird

T.A. Marryshow Community College

Information Technology (IT1A)

English and Communication 11 (COM 121)

31st March 2024

The Effect of Cyber Security Attacks on People’s Lives

In a world where technology is advancing, people are becoming too inclined with it and are using it to harm others. I am going to explain the effects of Cyber Security Attacks on people, who are the most vulnerable, what are some of the methods that hackers use to steal data and information, how does it affect the person that is targeted by these attacks, how common these attacks occur, and what are some of the ways in preventing these attacks in the future.

As money becomes an essential item in our economy, we tend to be more at risk whether it’s online or in-person. As we are discussing the impacts that cyber security has on people’s lives, a huge problem is the financial stability of the individual. According to (Elestedt, Nilsson, & Rosenvinge, 2021), it states that at the center of the financial system are payment systems and other financial market infrastructures. These systems are connected to banks, and they shaped the foundation of the financial system. The starting point of a cyber-attack is when the hacker or exploiter systematically targets the financial companies themselves or the third-party suppliers to the financial sector such as software, cloud services, energy supply and communication. If any hacker or exploiter gains any access to these information or details, the companies and banks can suffer a huge loss of customers and the economy will fall. That’s why the financial system depends on critical information in which it’s needed to be highly protected from attacks. Confidentiality, integrity, and availability are the three things that constantly occur when it comes to cyber security and protecting information. An example of this is with a Ukrainian ransomware attack called “NotPetya”, where this attack affected about ten percent of the computers and companies like banks and other financial institution and even as far as spreading beyond its borders. To protect companies and customers data, according to (Mathis, 2023), they adopt a data governance strategy which helps companies manage information across departments. This strategy aligns with the organization’s extensive growth plans, so the leadership teams must finalize it before implementation. Another way in which companies protect customers data is to limit who has access to certain data. This is a very efficient way of protecting data because it gives certain team members within the organization full control or limited access to the crucial data within their database.

An individual can be targeted by hackers and exploiters in many ways. According to (Torrence, 2023), Individuals and organizations are under cyber-attack around the globe, and these are some of the methods that exploiters or hackers use to gain access to data illegally. A phishing attack is where the hacker or exploiter attempts to illegally gain sensitive information to utilize or sell the stolen information. (Cloudfare, n.d.). Some of the ways in which hackers use this method is by pretending to be an authorized person from a certain company sending a very professional email with a malicious link disguised as the company website to steal data or gain access to the targeted user’s device to cause chaos. Another method in which hackers use is through malicious sites such as porn sites. According to (Dkmedia, 2023), hacker can use porn sites to target vulnerable users such as teens and lonely aged men. They use methods like creating malicious ads in the form of sexual behaviors to entice the user into clicking on the ad. When the user clicks it, they tell them to input certain personal details like your name, date of birth, location, and credit card information. With all these methods that these hackers are using let us explain how to prevent these attacks.

Preventing these cyber-attacks is very simple and easy depending on what attacks were used on you and how you are being attacked by the hacker or exploiter. According to (Federal Trade Commission, n.d.), your email (typically Gmail) provides a feature called spam filters which keeps many phishing emails out of your inbox. But today’s technology hackers have become advanced and outsmarted the spam filter. The Federal Trade Commission recommends that you protect your computer and cellphone by using security software that updates the software automatically so it can deal with any new security threats. They also recommend that you use multi-factor authentication, a feature that offers an extra layer of security by requiring two or more credentials to log into your accounts. Also, it is recommended that you back up your data on your computer or cell phone to an external hard drive or in the cloud.

Another question that is most asked is “Who are targeted the most?”. Well according to (Total Defense, 2020), hackers target most of the elderly people and children. Elderly people struggle to use modern technology which really isn’t their fault as they went majority of their lives without ever knowing how to use the internet, which is a big plus for these hackers because they can easily trick them into giving up personal information. It is important that younger people urge their elderly family members to protect themselves online and unrequested phone calls. Another person that hackers target is children, which is one of the vilest things anyone can do. Children love being on the internet and playing games, so they create profiles with usually very weak passwords so they can play their games. Normally children buy in-game items with real money which requires the use of a credit card, typically from a parent or guardian. Hackers use this to their advantage to target and trick children into giving up certain information, which can be detrimental to the parents or guardian if the hacker has their credit card or bank account information.

To conclude this research paper, it is important that we as individuals do our part in protecting ourselves and our loved ones, especially the elderlies and children, from being targeted by these individuals who are there to cause chaos in this society.

# References

Cloudfare. (n.d.). *What is a phishing attack?* Retrieved from Cloudflare: https://www.cloudflare.com/learning/access-management/phishing-attack/

Dkmedia. (2023, Auguest 3). *How to Browse Porn Sites Safely Without Getting Hacked*. Retrieved from Medium: https://medium.com/@dkmedia4749/how-to-browse-porn-sites-safely-without-getting-hacked-1e043b1cd954#:~:text=Avoiding%20Malware%20and%20Phishing%20Attacks%20on%20Porn%20Sites&text=Be%20wary%20of%20suspicious%20links,sites%20can%20sometimes%20contain%20malw

Elestedt, L., Nilsson, U., & Rosenvinge, C.-J. (2021, May 19). *A cyber attack can*. Retrieved from RiksBank: https://www.riksbank.se/globalassets/media/rapporter/ekonomiska-kommentarer/engelska/2021/a-cyber-attack-can-affect-financial-stability.pdf

Federal Trade Commission. (n.d.). *How to Recognize and Avoid Phishing Scams*. Retrieved from Federal Trade Commission Consumer Advice: https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Mathis, S. (2023, May 19). *Top 10 customer data privacy best practices*. Retrieved from Tech Target: https://www.techtarget.com/searchcustomerexperience/tip/Top-customer-data-privacy-best-practices

Torrence, C. (2023, April 17). *How Do Hackers Enter Your System? Exploiting Vulnerabilities in 2023*. Retrieved from Cyber Tec Security: https://info.cybertecsecurity.com/how-do-hackers-enter-your-system-exploiting-vulnerabilities-in-2023

Total Defense. (2020, June 24). *Who do hackers target the most?* Retrieved from Total Defense: https://www.totaldefense.com/security-blog/who-do-hackers-target-the-most/