Cybersecurity Training & Awareness

SUMPTER, QUINTIN
CYSE495

The cyber world has become one of the most important pieces in evolution today with a large number of people taking advantage of all opportunities the cyber world has to offer. Individuals and groups usually use the cyber world as a form of expression for one's sense of style and character or to be vocal about political and other worldwide situations. Organizations may use the cyber world to monitor product sales, customer satisfaction ratings, and pass along important information to one another. Many benefits have come from the cyber world but, there has also been an increase in many risks. Hackers can infiltrate user systems and gain access to all sensitive information without any consent and sometimes without the user's knowledge. Cybersecurity also is not simply applied to fighting against hackers but, is applied to protecting all within the cyber world. The cyber world is just as big if not bigger than the earth itself which leaves the chance for much room for unimaginable growth while sadly also creating new unwanted exploits soon to be discovered and used against the innocent. Proper training and awareness of cybersecurity can help individuals and organizations better protect themselves along with their private information.

Cyberspace has become its own separate world where individuals can access information at the push of a button and provide entertainment through streaming services or websites such as YouTube, Netflix, and Hulu. The social media side of the cyber world allows individuals a large amount of freedom over how they express themselves through the use of social media posts on their profiles showing a unique style or to voice opinions on important worldwide events. Another reason for the large continuous increase in social media involvement is that many believe they can get rich quickly after viewing others who have risen to fame. With all the possible benefits of the cyber world, individuals will still face many cyber threats and cyber crimes among all who indulge in this side of life. From Children, teenagers, and adults to

businesses and organizations, each faces its own cyber threats while also sharing some of the same threats. Children and teens have become the most active on social media platforms such as Instagram, Twitter, TikTok, and Facebook so much so that they will get all worldwide news from these platforms instead of on actual television. The threat that comes with their huge involvement in cyberspace is cyberbullying through forms of intimidation, harassment, racial harassment, abuse, and sexual exploitation (Rahman et al., 2020). An alarming statistic from the Royal Malaysian Police even states that over the past few years 80% of rape cases have been related to friendships taking place within the cyber world. Many parents are not aware of the potential threats their children may face when they start to become active in the cyber world. Those on the receiving end of bullying can develop depression, anxiety, health complaints, and poor academic scores which can all lead to them processing suicidal thoughts.

The Cybersecurity and Infrastructure Security Agency defines cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information". This is a standard definition of cybersecurity and many would only observe the obvious point that is being made which is that their important and private information would be protected. In truth all who use the network are to be protected in the cyber world whether it be from hackers attempting to exploit secret company files, infiltrating people's bank accounts, or those harassing another individual online. There have been plenty of measures taken by social media platforms to limit as many hateful acts as possible through monitorization of social media posts, comment sections, and allowing their customers to report someone for breaking community guidelines. These are the measures taken so that cyberbullying and other indecent behaviors can be monitored and put to a halt. It would also be important to prioritize teaching children the importance of password safety

among social media accounts and how to be aware of obvious scams from untrustworthy accounts. Though a child may not own a credit card, a hacker can still find a use for whatever ever else may be on their devices such as contacts and pictures. A mobile app called “Cyber Aware” developed by Filippos Giannakas, Georgios Kambourakis, and Stefanos Gritzalis was designed to properly educate children on the importance of cyber awareness (Quayyum et al., 2021). This is accomplished through game-based teaching within the mobile app being useful to all children in the range of kindergarten to early middle school life. Getting an early start on developing a cyber education can come in handy for a person’s future as they grow older developing more information they would rather keep private.

The same can be said for adults and businesses as they tend to deal with more threats targeting their internal systems and confidential information. Hackers come in many forms with some being professional hackers who receive payment to infiltrate systems and others being common criminals or “script kiddies” who depend on the research and tools of others (CISA, n.d.). Hackers can be quite clever and do careful planning in orderly steps to get the best results out of their infiltration attempts. Identifying vulnerabilities, scanning and testing network vulnerabilities, gaining access, and finally being sure to maintain that access (Esteves et al, 2017). Each step plays a vital role for hackers when infiltrating systems for their personal gain and being aware of these methods can help someone develop the mindset of a hacker so they may think like one of them and anticipate potential threats. As an individual, doing the bare minimum among cyber practices to ensure safety can have a larger impact on a person’s information safety. Steps to keep in mind for better cyber practice would be frequently using secure emails, changing passwords regularly, backing up all sensitive data, detecting and avoiding phishing emails, and using two-factor authentication software. This simple rotation of

practices can aid in the prevention of unwanted infiltration and in the worst-case scenario, helps lessen possible damages and data lost during the attack. These practices still apply to organizations as well but, to properly develop a trustworthy business there will be more in-depth qualifications met to ensure company and consumer safety.

With the recent coronavirus lockdown in the year 2020 and the pandemic still being at large two years later, maintaining good cybersecurity practices has become increasingly important with the amount of time many people have begun to spend inside and being required to work from their homes. These cybersecurity practices can also be referred to as maintaining good "cyber hygiene" and they are meant to be practiced regularly to better keep defenses up to date. These practices of cyber hygiene are as stated:

• Protecting all the cyberattacks and risks associated with internal and external suppliers;

•Addressing and preventing threats;

• Classifying business assets and services;

• Responding to business risks by establishing the proper response plan;

• Providing training and education about cybersecurity;

• Establishing constant monitoring of the network and accessing control that accommodates all user privileges;

• Having standardized configurations that will help to protect and recover data; and

• Monitoring the cyber threats (Ncubukezi & Mwansa, 2021).

What has not changed as a result of the pandemic is the amount of loss a business can suffer from insufficient cybersecurity practices. The advancement in technology has continued to grow

at an alarming rate which also allows for new developments in possible cyber threats. In the article “Business Organization Security Strategies to Cyber Security Threats” Bandr Fakiha (2021) stated, “According to Flores et al., cyber-attacks have the potential to influence both large and small business organizations, resulting in a range of financial consequences such as data theft, manipulation, and corruption. These risks ultimately interfere with the organization's brand, leading to a poor reputation and decreased competition in the financial markets”. Organizations are expected to maintain a higher level of cyber training and awareness since they have everything to lose from not having proper practice.

The evolution of technology has helped develop a second world that is separate and yet still united with the real world. The cyber world is where many have begun to feel most comfortable with expressing who they really are inside and exploring like-minded communities. With all the good coming from advanced technology also follows the bad side such as hackers and cyberwarfare. Hackers would be used in cyberwarfare as countries look to infiltrate one another’s files looking for any sensitive information but, there are the common hackers simply looking to take advantage of their fellow civilians who are more than likely obviously to the use of proper cyber hygiene. Having cybersecurity training and awareness does help in recognizing threats so that a person or company can better protect their private data but, cybersecurity also is about having those living their second life within the cyber network feel safe and protected. Cybersecurity is not only used when being hacked, instead applies to all activities within the cyber world to make the network enjoyable and safe for everyone.

REFERENCES

Alruwaili, A. (2019). A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science, 10*(5), 1–3. https://doi.org/10.26483/ijarcs.v10i5.6476

Cyber threat source descriptions. CISA. (n.d.). Retrieved August 6, 2022, from https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions#hacker

Esteves, J., Ramalho, E., & De Haro, G. (2017). To Improve Cybersecurity, Think Like a Hacker. *MIT Sloan Management Review, 58*(3), 71-77. http://proxy.lib.odu.edu/login

Fakiha, B. (2021). Business Organization Security Strategies to Cyber Security threats. *International Journal of Safety and Security Engineering*, *11*(1), 101–104. https://doi.org/10.18280/ijsse.110111

Giannakas, F., Kambourakis, G., & Gritzalis, S. (2015). CyberAware: A mobile game-based app for cybersecurity education and Awareness. *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*. https://doi.org/10.1109/imctl.2015.7359553

Ncubukezi, T., & Mwansa, L. (2021). Best practices used by businesses to maintain good cyber hygiene during covid19 pandemic. *Journal of Internet Technology and Secured Transactions*, *9*(1), 714–721. https://doi.org/10.20533/jitst.2046.3723.2021.0086

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

Rahman, N. A., Sairi, I. H., Zizi, N. A., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Security tip (ST04-001). CISA. (n.d.). Retrieved August 6, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST04-001