Social Media impacts on Cybersecurity

Amira Muaket

Old Dominion University

CYSE-280

Professor Malik A Gladden

December 2, 2024

“5.17 billion people use social media worldwide, according to platform reports on the current number of active users”(“Backlinko, 2024), with the growth of social media, has a severe impact on users. Popular social media platforms including Facebook, TikTok, Instagram, Linkedin, etc are powerful tools used to connect, promote, influence, engage, and entertain. With the excitement of sharing your activities, feelings, locations, or engaging with other people, many people don't realize that they contribute to critical cybersecurity risks. Since the introduction of social media, many users have been unaware of online dangers, leaving them exposed and vulnerable to numerous cyber risks/attacks. Cybercriminals will use strategies such as social engineering, harassment, bullying, data theft, etc to exploit their victims. Once understanding the major cybersecurity concerns and how hackers use their instruments to cause detrimental damage. One can follow respective frameworks, protocols, and tools to counteract these threats by reviewing and analyzing the latest cybersecurity trends. Overall, fully comprehending the impacts that social media has on cybersecurity is essential.

The role of social media is deeply embedded in today's society. It was created to allow individuals to communicate easily, express opinions and ideas, share news, and to promote businesses. There are positive and negative effects of social media usage, such as on mental health, education, businesses, and overall “society”. “A Study on Positive and Negative Effects of Social Media on Society” by Waseem Akram, discusses social media's influence on society in a broader scope. One of the main positive attributes discussed was its influence on connectivity (the ability to connect to multiple users), education (specifically for students and teachers as one can enhance their knowledge through various fields), and advertising (promoting businesses to large audiences and informing the public of many innovations as a way to increase profit). On

the other hand, there are negatives when it comes to social media usage and the study focuses on certain attributions, such as cyber harassing (terrorizing or tormenting individuals or groups through hateful or threatening messages), hacking (manipulating or stealing personal information, and breaching security, “Some twitter and Facebook accounts have been hacked in the past and the programmer had posted materials that have influenced the person's lives”(Akram, pg.352, 2017)), and fraud/scam (tricking individuals into offering financial information to take advantage of).

Once understanding the role of social media in society, one can recognize how cyber threats/attacks originate from social media. One of the biggest threats to social media is “social engineering” attacks, which is a tactic used to impersonate or manipulate users into gaining control over their platforms. This can include the ability to steal personal and financial information. “Social engineering, due in part to the increasing popularity and advancements in information technology and ubiquity of devices, has emerged as one of the most challenging cyber security threats in the contemporary age.”(Aldawood and Skinner, 2018). Some other methods of cyber attacks are implemented through phishing attacks (using messages, emails, or websites to trick users into sharing personal data, downloading malicious links, or exposing themselves to cybercrimes), data theft (stealing digital data that is stored in one's digital devices, such as computers, phones, tablets, etc.), malware (programs that intercept a system, such as worms, viruses, trojans, spyware, etc), and impersonations (the use of fake names or posing as someone to trick consumers). These are some of many techniques that attackers use to reach their goal, whether for financial gain, accessing unauthorized data, or just for the thrill of it, it's always best to be always cautious.

Data breaches, especially in social media are a huge problem as well. We can examine the Facebook breach that occurred in 2021, where 533 million users were affected. Hackers decided to hack Facebook by discovering vulnerabilities within the system and exploiting them. Allowing them access to millions of users' information including " full names, phone numbers, locations, and birthdates of Facebook users."(Twingate Team, 2024). This is one of many privacy/data breaches that occur in social media, as technology advances there has been an increase of these instances happening. In the study "The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence" the authors point out that the problem of data breaches is not going away and consumers must understand the severity of this issue. "In a survey conducted by Pew Research, a majority of Americans (64%) have personally experienced a major data breach and lack trust in key institutions"(Ho et al., 2023). This current problem and other incidents highlight design flaws and faulty systems due to weak security practices.

This raises concerns about social media vulnerabilities, especially the lack of cyber hygiene. Many individuals lack awareness in the cyber sense, meaning they don't incorporate cybersecurity practices into their daily lives. For instance, having weak passwords can lead to cybercriminals gaining unauthorized access. Excessively oversharing online like locations, employment, and school/university you attend can lead to identity theft. Sharing opinions, photos, beliefs, and so on, can give one insight into cyberbullying, stalking, or harassment. Small instances like this used in a social media space can increase the risk of becoming a cyber victim. A study was conducted at "Imam Abdulrahman Bin Faisal University", where Mohammed A.

Alqahtani conducted a survey revolving around cybersecurity awareness such as passwords, browsers, and social media security. Received 450 responses and indicated that many students had minimal knowledge concerning “password security” practices. “Students’ levels of cybersecurity awareness are still lacking, especially when it comes to password security. Students usually do not pay much attention to using good and correct passwords to protect their accounts or websites.”(Alqahtani, 2022).

It's especially important to shed light on user awareness. Following the correct frameworks and incorporating cybersecurity practices can enhance one's knowledge and awareness concerning cybersecurity. Once a user understands the threats that come with social media, users can reduce the risk of becoming victims of cybercrimes. It will improve people's livelihood and enjoy using social media without having to worry about the dangers online. Some methods one can follow is the social media security process. It's a set protocol one can use to protect themselves when indulging in social media. “It provides security against online harassment, unauthorized access, phishing attacks, malware, data breaches and identity theft.”(Suresh, 2024). Some simple steps that users, groups, businesses, and organizations can adapt to are efficiently implementing strong passwords, by adding numbers, capitalized letters, and special characters. Enabling two-factor or multi-factor authentications on social media applications can enhance security. Regularly update applications software or privacy settings so attackers won't take advantage of them. Don't accept friend requests from random people you don't know, even if the requester displays “friends in common”, it can be a manipulation tactic used by attackers. Be extremely cautious what you post on social media, since attackers can use that information for personal gain. Pay attention in connecting to free public Wi-Fis, since these

are usually not secured, making it easier for hackers to intercept data. Regarding business/organizations or for children, imply access controls, as this can limit privileges ensuring data and information are kept safe and secured. And the most important practice is always keeping yourself and others educated!

Tools or resources users and businesses can find or use are reading or following cybersecurity trends. Understanding the need for cybersecurity from studies, statistics, demographics, etc can enhance one's mindset and the scope of the problems. Businesses can incorporate the NIST (National Institute of Science and Technology) cybersecurity frameworks, as it was designed to provide different guides through publications on how to understand and manage different cybersecurity risks. NIST does offer a special publication that covers social media in the workplace. It's the 800-53, Revision 5 called “Social Media And Networking Restrictions”, and it includes “the rules of behavior, explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.”(NIST). Offering a wide range of alternative practices for various cybersecurity scenarios one may encounter. As well as imposing a set of rules and regulations on a workplace that a business can include depending on their priority levels and objections. For regular users one can search for different techniques or materials one can use, for example, websites such as CISA or TechTarget offer the latest news regarding cybersecurity incidents and ways to prevent them. As well as software or products one can download onto their system. For instance, using ad blockers systems to prevent malicious pop-up ads. On TechGate, there's this interesting article called “17 free cybersecurity tools you should know about” since cybersecurity applications can be quite

pricey. It's a great resource to take advantage of because not only can you use these tools for social media, you can also apply them for other devices, softwares, and applications.

With the rapid growth of technology, we can examine how cybersecurity has transformed how we connect through social media. Highlighting the different challenges that are associated with social media, such as social engineering tactics, cyberbullying/harassment, identity theft, data breaches, and so on is crucial. By grasping the complexities of the risks one can engage in social media security protocols, providing safe alternatives and practices when communicating online, as well as, implementing various tools. I also want to point out the critical need for enhancing one's cyber hygiene. In order for businesses and users to ensure their privacy and data are secure, education is key for user awareness. Adopting various training modules or reading the latest cybersecurity trends is an efficient way to spread knowledge of these important situations. Not to mention, adding key procedures from popular publications such as NIST can easily combat cybercriminal activities. Overall, we must place importance on social media safety by continuing research since there is always going to be a problem emerging from such applications. The growth in technology is also a growth in cyber-related incidents from various perspectives.

References

Akram, W., & Kumar, R. (2018, March). A Study on Positive and Negative Effects of Social Media on Society. ResearchGate. https://www.researchgate.net/publication/323903323_A_Study_on_Positive_and_Negative_Effects_of_Social_Media_on_Society

Chang, V., Golightly, L., Xu, Q. A., Boonmee, T., & Liu, B. S. (2023). Cybersecurity for children: an investigation into the application of social media. Enterprise Information Systems, 17(11). https://doi.org/10.1080/17517575.2023.2188122

Chin, K. (2023, May 8). The Impact of Social Media on Cybersecurity | UpGuard. Www.upguard.com. https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity

Dean, B. (2024, February 21). How Many People Use Social Media in 2022? (65+ Statistics). Backlinko. https://backlinko.com/social-media-users#

Ho, F. N., Ho-Dac, N., & Huang, J.-H. (2023). The Effects of Privacy and Data Breaches on Consumers' Online Self-Disclosure, Protection Behavior, and Message Valence. SAGE Open, 13(3). sagepub. https://doi.org/10.1177/21582440231181395

Khidzir, N. Z., Ismail, A. R., Daud, K. A. M., Ghani, M. S. A. A., & Ibrahim, M. A. H. I. (2016). Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements. Lecture Notes on Information Theory, 4(1), 18–24. https://doi.org/10.18178/lnit.4.1.18-24

Kosinski, M. (2024, May 17). What is phishing? IBM. https://www.ibm.com/topics/phishing

Aldawood, H., & Skinner, G. (2018, December 7). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Researchgate; IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE).

https://www.researchgate.net/profile/Hussain-Aldawood/publication/330293734_Educating_and_Raising_Awareness_on_Cyber_Security_Social_Engineering_A_Literature_Review/links/5d9ae3c192851c2f70f21bf8/Educating-and-Raising-Awareness-on-Cyber-Security-Social-Engineering-A-Literature-Review.pdf

Nik Zulkarnaen Khidzir, Rasdan, A., Azhar, K., Daud, M., & Mohd. (2016). Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements. The 2016 5th International Conference on Software and Information Engineering (ICSIE 2016). https://www.researchgate.net/publication/303444261_Critical_Cybersecurity_Risk_Factors_in_Digital_Social_Media_Analysis_of_Information_Security_Requirements

Social Media And Networking Restrictions - CSF Tools. (2020, August 13). CSF Tools - the Cybersecurity Framework for Humans. https://csf.tools/reference/nist-sp-800-53/r4/pl/pl-4/pl-4-1/

Taylor, H. (2021, June 16). What Are Cyber Threats and What to Do About Them | Prey Blog. Preyproject.com. https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them

Twingate Team. (2024, February 22). What happened in the Facebook data breach? | Twingate. Www.twingate.com. https://www.twingate.com/blog/tips/facebook-data-breach

10 Best Practices for Social Media Security: Pro Tips. (n.d.). Www.sprinklr.com. https://www.sprinklr.com/blog/social-media-security-best-practices/#toc-2

17 free cybersecurity tools you should know about. (n.d.). WhatIs.com. https://www.techtarget.com/whatis/feature/17-free-cybersecurity-tools-you-should-know-about