SOCIAL MEDIA AND CYBER SECURITY: PROTECTING AGAINST ONLINE THREATS AND ATTACKS

Conference Paper · August 2023

CITATIONS
0

READS
1,099

2 authors:

Ahmed Buhari
National institute of construction technology and management
5 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Zayyad Isa
National Institute of construction technology, Uromi
6 PUBLICATIONS **79** CITATIONS
SEE PROFILE

SOCIAL MEDIA AND CYBER SECURITY: PROTECTING AGAINST ONLINE THREATS AND ATTACKS

Authors:

1. **Ahmed Buhari**

a.buhari@nict.edu.ng | *08036322058*

Department of Computer Science, National Institute of Construction Technology and Management (NICTM) Uromi, Edo State.

2. **Zayyad Isa Sulaiman**

z.isa@nict.edu.ng | *07062887127*

Department of Computer Science, National Institute of Construction Technology and Management (NICTM) Uromi, Edo State.

Abstract:

A new wave of online threats and attacks has been brought on by the growth of social media. Individuals and companies are becoming increasingly vulnerable to internet risks, such as bullying, data theft, identity theft, and phishing scams. This paper investigates the numerous effects of social media on cyber security and looks at defence mechanisms that could be used to safeguard against these security threats. We'll also discuss how crucial User Awareness and Education are to preserving cyber security.

Introduction

Social media has transformed how people communicate with one another and has emerged as a crucial tool for organisations, governments, and people. Oberlo (2021) estimates that there are already more than 4.2 billion social media users globally, and that number is predicted to increase to 4.4 billion by 2025. However, as social media platforms are used more frequently, there is also a higher danger of cybersecurity issues, such as identity theft, cyberbullying, hacking, phishing, and other cyber attacks.

This paper explores the precautions that people and organisations can take to safeguard themselves against online threats and attacks. It also examines the potential risks related to social media use. The study also looks at how governments and social media businesses can promote cybersecurity awareness and practice.

Social Media and cybersecurity

Cybercriminals frequently target social media sites because of the enormous amount of personal information that users provide online. This data can be used by cybercriminals to undertake identity theft, phishing, malware, and social engineering assaults, among other types of attacks.

Identity Theft happens when someone steals a victim's personal information displayed on the social media account and uses that information claiming to be the victim. **Phishing attacks** entail sending phoney emails or messages that seem to be from a trustworthy source with the intention of collecting personal data like passwords and credit card numbers. **Malware attacks** happen when Malicious software that can steal information or take control of the user's device is introduced onto the device through various means such as pictures sent to social media accounts. **Social engineering attacks** on the other hand entail persuading consumers to click on a malicious link or divulge private information.

Relationship between Social Media and Cybersecurity

Social media platforms have gained popularity among users because of their distinctive communication and engagement characteristics. However, because users disclose so much private information online, these platforms have also become targets for fraudsters. This information is used by online criminals to launch a variety of assaults, such as phishing,

malware, and social engineering attempts. Since social media platforms operate in a dynamic environment with continuously changing dangers and threats, social media also poses a challenge for cybersecurity specialists.

Impact of Social Media on Cybersecurity

Social media sites have become a gold mine for hackers. A variety of targeted attacks, including phishing scams, malware infections, and identity theft, can be launched using the huge amount of personal information posted on these platforms, such as email addresses, phone numbers, and geographical information. These details can be used by cybercriminals to create communications that are incredibly convincing and seem to come from reliable sources, duping users into disclosing critical information. In addition, false accounts and profiles have flourished on social media sites, where they can be exploited to transmit malware and steal private information.

Potential Risks Associated with Social Media Use

The use of social media carries a number of possible hazards and threats that may have varying effects on people and organisations. The following are some of the most typical hazards connected to using social media:

1. Identity theft: Since social media platforms frequently ask users to provide personal information; fraud, and identity theft are two crimes that cybercriminals might perform using this information (Sacco & Carvey, 2019).
2. Cyberbullying: Social media provides a forum for individuals to engage in bullying and harassment, which can have serious psychological and emotional impacts on victims (Kowalski & Limber, 2013).
3. Hacking: Social media accounts are frequently targeted by cybercriminals who can exploit them to acquire private data and launch additional cyberattacks (Sridhar, 2019).
4. Phishing: Cybercriminals frequently utilise social media to conduct phishing attacks, in which they create phoney websites and emails in an effort to collect sensitive data (Cooke, 2019).

Common Types of Cyber Attacks

Social Media Cyber Attacks come in several types and scenarios. Phishing attacks occur when cybercriminals use phoney emails or messages to deceive victims into disclosing personal information like passwords or credit card numbers. The use of malicious software to infect users' devices with software intended to steal information or take control of the device is known as a malware attack. Attacks using social engineering manipulate users to gain access to systems, data, or sensitive information. Any social media platform might be the target of these attacks, so users need to be aware of these attacks and be proactive in protecting themselves.

Protecting Against Online Threats and Attacks

Individuals and organisations must adopt a proactive cybersecurity strategy in order to safeguard against online dangers and attacks. Implementing multi-factor authentication, which provides an additional layer of security to user accounts, is one viable technique. This can aid in limiting unauthorised access to sensitive and personal data (Primary technology, 2023). Regular software and security patch updates are another crucial tactic that can aid in preventing vulnerabilities that cybercriminals could exploit.

The maintenance of cybersecurity also requires user education and awareness in addition to technical solutions. The recommended practices for online security, such as avoiding dubious links and communications and often changing passwords, should be explained to users in order (Al-Janabi & Al-Shourbaji, 2016) to make sure that staff are informed about the most recent risks and are equipped to handle them; organisations can also develop security training programs for them.

Individuals and organisations can use a variety of ways to defend themselves against online threats and attacks, such as:

1. Strong passwords: Users should create separate passwords that are both strong and unique for each of their social media accounts (Hossain et al., 2021).
2. Two-factor authentication: Users have the option to enable two-factor authentication on their social media accounts, which provides an additional layer of protection by requiring a second verification step, such as a code texted to a mobile device (Chen et al., 2019).

3. Be Cautious When Clicking on Links: Users should be careful when clicking on links, especially if they are not sure of the source. Malicious links can infect a user's device with malware or redirect them to a phishing site.
4. Keep Software Up to Date: Software should be updated regularly to patch security vulnerabilities. This includes operating systems, antivirus software, and web browsers.
5. Limit Personal Information Sharing: Users should be cautious about the amount of personal information they share on social media platforms. They should avoid sharing sensitive information such as their home address, phone number, or financial information.
6. Privacy settings: Social media platforms have a range of privacy options that can be used to limit access to personal data and stop cybercriminals from gaining access to sensitive information (Sacco & Carvey, 2019).
7. Be Vigilant: Users should be vigilant and report any suspicious activity or messages to the platform's support team. They should also monitor their accounts regularly for any unauthorised access.

Role of Social Media Companies and Government Bodies

Social media firms should take precautions to shield their consumers from online threats and attacks since they have a crucial role to play in guaranteeing cybersecurity. Some of the precautions social media companies can take are as follows:

1. In order to protect user data, social media organisations can employ encryption (Tudor, 2018). This makes it more difficult for cybercriminals to access private data.
2. User education: According to Krumholz et al. (2017), social media firms can offer users educational materials and advice on how to safeguard themselves against online dangers and attacks.
3. Strong cybersecurity rules that prioritise user safety and defend against online dangers and attacks should be implemented by social media organisations, according to Panday and Chatterjee (2019).

Government entities can play a part in maintaining cybersecurity by, among other things, taking the following actions:

1. Regulation: Social media firms may be subject to government regulation, including requirements that they adhere to cybersecurity standards and directives (Kshetri, 2018).
2. Public education: According to Nurmi and Weir (2018), governments can raise the general public's knowledge of online hazards and provide information on how to defend against cyberattacks.
3. Collaboration: To create and execute cybersecurity measures that safeguard users and thwart online threats and assaults, governments can work with social media firms (Holt & Kilger, 2017).

Conclusion

Social media has ingrained itself deeply into our daily lives, but it has also created fresh cybersecurity challenges. Cybercriminals are launching targeted assaults and stealing sensitive data by using a large amount of personal information available on social media. People and organisations need to adopt a proactive approach to cybersecurity in order to guard against these dangers. This includes putting technical solutions into place and instructing people on the best practices for online security. By doing this, we can contribute to keeping our online activities safe and secure.

References:

1. Al-Janabi, S., & Al-Shourbaji, I. (2016, January 29). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(1), 30. http://dx.doi.org/10.1142/S0219649216500076
2. Chen, C.-W., Hsu, C.-Y., & Lin, H.-T. (2019). The impact of two-factor authentication on the intention to continue using social network services: An empirical study. *Journal of Computer Information Systems, 59*(3), 278-287.
3. Cooke, A. (2019). Phishing on social media: Risks and preventative strategies. *Journal of Cybersecurity, 5*(1), 1-12.
4. Holt, T. J., & Kilger, M. (2017). Social media and policing: An overview. *In The Routledge Handbook of Technology, Crime and Justice* (pp. 131-145). Routledge.
5. Hossain, M. S., Uddin, S., Islam, M. M., & Rashid, R. A. (2021). Social media security and privacy: A systematic review. *International Journal of Information Management, 57*, 102294.

6. Kowalski, R. M., & Limber, S. P. (2013). Psychological, physical, and academic correlates of cyberbullying and traditional bullying. *Journal of Adolescent Health, 53*(1), S13-S20.
7. Krombholz, K., Merkl, D., Weippl, E. R., & Zimmerman, S. (2017). A longitudinal measurement study of TCP/IP fingerprint-based classification. *ACM Transactions on Privacy and Security (TOPS), 20*(4), 1-26.
8. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management, 39*, 80-89.
9. Nurmi, C. E., & Weir, R. A. (2018). Government responses to cyber security threats: The impact of public opinion on policy. *Journal of Homeland Security and Emergency Management, 15(*1), 1-15.
10. Oberlo. (2021). *Social media marketing statistics.* Retrieved from https://www.oberlo.com/statistics/social-media-marketing
11. Pandey, V., & Chatterjee, M. (2019). *A review of social media security and privacy risks: Current trends and future research directions. Telematics and Informatics, 39,* 56-77.Sacco, D., & Carvey, H. (2017). Investigating cybercrime: Digital forensics in the 21st century. Syngress.
12. Primary technology. (2023, February 7). *When and why to use Multi-Factor Authentication*. Primary Technology. Retrieved May 10, 2023, from https://primaryt.co.uk/when-to-use-multi-factor-authentication/
13. Siddiqui, M. Z., Rahman, Z., & Hussain, I. (2020). Social media users' privacy and security concerns: A comprehensive review of existing literature. *Journal of Information Privacy and Security, 16*(1), 18-38.
14. Statista. (2021). *Number of social media users worldwide from 2010 to 2026*. Retrieved from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
15. Wang, C.-H., Chen, K.-C., & Lin, J.-S. (2019). Privacy concerns, trust in government, and behavioural intentions of social media users: A study of Chinese Weibo users. *Journal of Information Privacy and Security, 15*(1), 31-42