Cybersecurity Practices for Social Media Users

Subjects: Computer Science, Artificial Intelligence

Contributor: Thilini Herath

Cybersecurity is a collection of technologies established to protect the cyber environment of an individual user or organization. There are many cyber threats existing within the social media platform, such as loss of productivity, cyber bullying, cyber stalking, identity theft, social information overload, inconsistent personal branding, personal reputation damage, data breach, malicious software, service interruptions, hacks, and unauthorized access to social media accounts. It is also revealed that demographic factors, for example age, gender, and education level, may not necessarily be influential factors affecting the cyber awareness of the internet users.

Keywords: cybercrimes ; cyber threats ; cybersecurity ; cyber awareness ; Cyber behavior ; social media

1. Introduction

The internet has become one of the primary communication channels in the modern era and social media possess a large portion of internet usage ([1] Bosse, Renner, and Wilkens, 2020). A total of 3.78 billion users are predicted to have used social media in 2021 ([2] Tankovska, 2021 January 28). Most countries have acknowledged that cybersecurity has become one of the most critical issues that has emerged in the past few years with the increased usage of internet and social media ([3] Tosun et al., 2020). This might be due to the fact that high social media usage has become a new trend, reaching a wide range of people within a short time period ([4] Constantinides and Stagno, 2011; as cited by Okyireh and Okyireh, 2016). Additionally, the number of and types of available social media platforms, their less reliable design and construction, the large unstructured content, and more opportunities provided for people to act in malicious ways in those platforms have triggered the vulnerability of high-level cyber threats in social media ([5] Chaffey, 2016; Haimson and Hoffmann, 2016; Assunção et al., 2015; Fire et al., 2014; as cited by van der Walt, Eloff, and Grobler, 2018).

2. Cyber Threats on the Internet

The evolution of cybercrimes in the IT industry dates back to late 1970s. It has evolved from just spam at that time to much more advanced forms, such as viruses and malware, in the present day ([6] Jobs, 2016; as cited by Kruse, Frederick, Jacobson, and Monticone, 2017). The word “Cybercrimes” covers a vast range of virtual illegal activities performed by cybercriminals via any source of internet-connected electronic device ([7] Ali, 2019). Experts say that cybercriminals often aim for easy targets with the least resistance, even though they possess many sources, as well as a high level of knowledge on how the technology works and its vulnerabilities. The reason for this is that they can easily commence the hacking with less effort with that kind of user ([8] Shryock, 2019). Gullible users often become targets of hackers and cybercriminals use creative and different ways to collect personal data from them ([9] Ramakrishnan and Tandon, 2018). The internet has become an essential part of society and it has become the core of connecting and sharing information in modern days. This has led the internet to become a target of various cyber threats, ranging from cybercrimes (hacking, identity theft, and other forms of fraud) to cyber espionage, cyber terrorism, and cyber warfare ([10] van den Berg and Keymolen, 2017). Cybercrimes cover various cyber threats, including child pornography, fraud, email abuse, missing children, stalking, copyright, violation, harassment, threats, children abuse hacking, viruses, and many more ([11] Tripathi, Tripathi, and Yadav, 2016). The impact of cyber threats is changing, based on globalization, imposed security environment level, awareness, and the education level of the administrators and users of a given information and communication environment. These cyber threats can range from privacy, personal, confidential, and classified data loss and fund/cryptocurrency loss to harm to the health and/or life of a person ([12] Svoboda and Lukas, 2019).

3. Cyber Threats on Social Media

There are two major categories of social media risks. One is social risk and the other is technology risk. Social risks further branch into two categories, namely individual-level risk and professional-level risk. Loss of productivity, cyberbullying, cyberstalking, identity theft, and social information overload belong to individual-level risks, while

inconsistent personal branding, personal reputational damage, and data breach belong to professional-level risks. Technology risks mainly include malicious software, service interruptions, hacks, and unauthorized access to social media accounts ([13] van Zyl, 2009; Krasnova et al., 2009; Hogben, 2007; Krasnova et al., 2009; Boyd, 2008; Argenti and Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Hogben, 2007; Rivera et al., 2015; as cited by Goh, Di Gangi, Rivera, and Worrell, 2016). Cracking a password becomes easy for a hacker who possesses the right software tools and a few personal data, gained from someone's social media ([14] Eddolls, 2016). Fake accounts, cyberbullying, and sexual harassment are some of the major malicious behaviors that can be identified within the social media sphere ([15] van Schaik et al., 2017). Various cyberattacks are present in social media, such as identity theft, spam attacks, malware attacks, Sybil attacks, social phishing, impersonation, hijacking, fake requests, and image retrieval and analysis ([16] Zhang and Gupta, 2018). Additionally, social media has become a major playground for spear phishing attacks ([17] Bossetta, 2018) and social engineering ([18] Wilcox, Bhattacharya, and Islam, 2014; as cited by Aldawood and Skinner, 2019).

4. Cybersecurity on the Internet

Cybersecurity is a collection of techniques that have been established to protect individual users' or organizations' cyber environments ([19] Seemma, Nandhini, and Sowmiya, 2018; as cited by Richardson, Lemoine, Stephens, and Waller, 2020). A cybersecurity culture protects information systems, computer networks, user data, and internet users effectively ([20] Patrascu, 2019). Most of the cyber attacks are preventable or at least can be handled carefully; although, there is no perfect defense against them ([21] Kenyon, 2018; as cited by Bayard, 2019).

5. Cybersecurity on Social Media

Social media is a collection of electronic communication platforms used by online users to create online communities. They use these platforms to share information, ideas, and personal messages with each other ([22] Bhatnagar and Pry, 2020). Social media networks provide openness to user profiles and the data they share in the profile. However, this openness threatens user profiles with being revealed or hacked ([23] Tang-Mui and Chan-Eang, 2017). Most of the social media users are now addicted to sharing their ideas, sentiments, and experiments with a wide range of friends and friends of friends, via videos and photos ([16] Yan, 2016; as cited by Zhang and Gupta, 2018). People who post information online might not think of security risks associated with it primarily. However, this action can voluntarily reveal more personal information to unknown people than they expected ([24] Nyblom, Wangen, and Gkioulos, 2020).

6. Existing Cyber Threats and Cyber Awareness

It was found that there are many cyber threats existing within social media platforms, such as loss of productivity, cyberbullying, cyberstalking, identity theft, social information overload, inconsistent personal branding, personal reputational damage, data breach, malicious software, service interruptions, hacks, unauthorized access to social media accounts ([13] van Zyl, 2009; Krasnova et al., 2009; Hogben, 2007; Krasnova et al., 2009; Boyd, 2008; Argenti and Druckenbiller, 2004; Aula, 2010; Boyd, 2008; Hogben, 2007; Rivera et al., 2015; as cited by Goh et al., 2016), cracking a password ([14] Eddolls, 2016), fake accounts, sexual harassments ([15] van Schaik et al., 2017), spam attacks, malware attacks, Sybil attacks, impersonation, hijacking, fake requests, image retrieval and analysis ([16] Zhang and Gupta, 2018), spear phishing attacks ([17] Bossetta, 2018), and social engineering ([18] Wilcox, Bhattacharya, and Islam, 2014; as cited by Aldawood and Skinner, 2019).

All users should have enough current and updated cyber awareness and cyber behavior to safeguard themselves from the aforementioned cyber threats. Tragically, most users have failed to achieve an acceptable level of protection compared with the increasing rate of threats ([9] Ramakrishnan and Tandon, 2018). People who post information online might not think of security risks associated with this behavior. However, this action can voluntarily reveal more personal information to unknown people than they expected ([24] Nyblom et al., 2020). It is also revealed that most social media users are unaware of the risks and vulnerabilities associated with those platforms unless they have experienced those in their real lives ([25] Atiso and Kammer, 2018). Hence, it is always recommended that users take enough precautions to safeguard themselves from cybercrimes from their point of view, since the most powerful user privacy protection strategy in social media platforms falls into users' own hands. Only they can control what they publish, and to whom, on those platforms ([26] Pensa and Di Blasi, 2017).

When it comes to factors affecting cyber awareness, it was discovered that age, gender, and education level may or may not affect the cyber awareness of internet users. Older adults had higher information security awareness (ISA) scores than young adults. A small significant difference was found in the ISA score related to gender, where females had higher

ISA scores compared with males ([27] McCormac et al., 2017). In contrast to this citation, another research article stated otherwise, finding that males have more cyber hygiene knowledge than females; however, surprisingly, there was no difference in cyber hygiene knowledge among different age groups ([28] Cain et al., 2018). In the research, it was found that higher education levels lead to higher information security awareness of the users—higher education levels or information security training reduces risky user behavior ([29] Ogutcu et al., 2016). However, in a multinomial regression analysis, it was found that people with higher education and who are not living in their own housing are more likely to fall into the cybercrime victims category ([30] Oksanen, and Keipi, 2013, as cited by Nalaka and Diunugala, 2020).

Research results show that higher awareness was connected with a lower number of reported online risky behaviors ([31] Schilder, Brusselaers, and Bogaerts, 2016). Lack of understanding regarding appropriate cybersecurity actions can lead end users to inappropriate cyber behavior ([28] Debatin et al., 2009; Goodhue, and Straub, 1991; Hu, Hart, and Cooke, 2006; Straub, and Welke, 1998; as cited by Cain et al., 2018). The research findings revealed that user awareness improvements lead to better security behavior ([32] Furnell, Khern-am-nuai, Esmael, Yang, and Li, 2018). Security awareness impacts user behavior when protecting against risks in information security ([33] Herath, and Rao, 2009; Thomson, and Solms, 1998; Puhakainen, and Siponene, 2010; as cited by Torten, Reaiche, and Boyle, 2018). On the other hand, a study conducted by the Global Cybersecurity Capacity Centre at the University of Oxford found that campaigns on cybersecurity awareness were unsuccessful in changing behavior ([34] Bada et al., 2015; as cited by Chang and Coppel, 2020); additionally, they found that cyber behavior has an impact on the vulnerability level that users face. In another study, it was identified that the cybersecurity behavior of the respondents potentially makes them vulnerable to cyber threats ([35] Muniandy, Muniandy, and Samsudin, 2017).

7. Conclusions

Cybersecurity, within the context of social media, is a timely topic to be discussed considering its large user base all around the world. There are many cyberattacks existing in the current social media sphere. Although there is an in-built security framework within the different social media platforms, it may not be enough to protect the social media users from cyber attacks. This is due to human error, where there is the possibility of opening backdoors for commencing cyber attacks. User awareness and user behavior play a major role to reduce the impact of human errors. The impact of factors, such as age, gender, and the education level of the users on their cyber awareness in social media platforms' security features is not clear, based on the current literature found. However, the impact of cyber awareness over cyber behavior is backed by several studies. Additionally, there is not enough evidence to prove the impact of users' secured cyber behavior on their vulnerability level on social media platforms. Hence, further research is crucial to identify the factors affecting user awareness, users' secure behavior, and users' vulnerability level on social media platforms. Moreover, it is significant to discover recommended cybersecurity practices for social media users, based on the impact of the aforementioned variables.

References

1. Bosse, I.; Renner, G.; Wilkens, L. Social media and Internet use patterns by adolescents with complex communication needs. Lang. Speech Hear. Serv. Sch. 2020, 51, 1024–1036.
2. Tankovska, H. Number of Global Social Network Users 2017–2025. 2021. Available online: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/ (accessed on 10 January 2021).
3. Tosun, N.; Altinoz, M.; Cay, E.; Cinkilic, T.; Gulseçen, S.; Yildirim, T.; Aydin, M.A.; Metin, B.; Ayvaz Reis, Z.; Unlu, N. A SWOT Analysis to Raise Awareness about Cyber Security and Proper Use of Social Media: Istanbul Sample. Int. J. Curric. Instr. 2020, 12, 271–294.
4. Okyireh, R.O.; Okyireh, M.A.A. Experience of Social Media, Training and Development on Work Proficiency: A Qualitative Study with Security Personnel. J. Educ. Pract. 2016, 7, 122–127.
5. van der Walt, E.; Eloff, J.; Grobler, J. Cyber-security: Identity deception detection on social media platforms. Comput. Secur. 2018, 78, 76–89.
6. Kruse, C.S.; Frederick, B.; Jacobson, T.; Monticone, D.K. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol. Health Care 2017, 25, 1–10.
7. Ali, L. Cyber crimes—A constant threat for the business sector and its growth (A study of the online banking sector in GCC). J. Dev. Areas 2019, 53. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbig&AN=edsbig.A554041623&site=eds-live&scope=site (accessed on 12 January 2021).

8. Shryock, T. The growing cyber threat: Practices are increasingly coming under attack by cyber criminals. Med. Econ. 2019, 96, 22. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsgac&AN=edsgac.A590952666&site=eds-live&scope=site (accessed on 15 January 2021).
9. Ramakrishnan, U.P.; Tandon, J.K. The evolving lanscape of cyber threats. Vidwat Indian J. Manag. 2018, 11, 31–35. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139235797&site=eds-live&scope=site (accessed on 18 January 2021).
10. Van den Berg, B.; Keymolen, E. Regulating security on the Internet: Control versus trust. Int. Rev. Law Comput. Technol. 2017, 31, 188–205.
11. Tripathi, E.; Tripathi, A.; Yadav, M.K.S. Role of information technology in cyber crime and ethical issues in cyber ethics. Int. J. Bus. Eng. Res. 2016, 10, 1–5. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=139360194&site=eds-live&scope=site (accessed on 18 January 2021).
12. Svoboda, J.A.N.; Lukas, L. Sources of threats and threats in cyber security. DAAAM Int. Sci. Book 2019, 321–330. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=140062921&site=eds-live&scope=site (accessed on 18 January 2021).
13. Goh, S.H.; Di Gangi, P.M.; Rivera, J.C.; Worrell, J.L. Graduate student perceptions of personal social media risk: A comparison study. Issues Inf. Syst. 2016, 17, 109–119. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=119120441&site=eds-live&scope=site (accessed on 19 January 2021).
14. Eddolls, M. Making cybercrime prevention the highest priority. Netw. Secur. 2016, 2016, 5–8.
15. Van Schaik, P.; Jeske, D.; Onibokun, J.; Coventry, L.; Jansen, J.; Kusev, P. Risk perceptions of cyber-security and precautionary behaviour. Comput. Hum. Behav. 2017, 75, 547–559.
16. Zhang, Z.; Gupta, B.B. Social media security and trustworthiness: Overview and new direction. Futur. Gener. Comput. Syst. 2018, 86, 914–925.
17. Bossetta, M. The weaponization of social media: Spear phishing and cyber attacks on democracy. J. Int. Aff. 2018, 71, 97–106. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=132491875&site=eds-live&scope=site (accessed on 19 January 2021).
18. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet 2019, 11, 73. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=135682631&site=eds-live&scope=site (accessed on 1 February 2021).
19. Richardson, M.D.; Lemoine, P.A.; Stephens, W.E.; Waller, R.E. Planning for cyber security in schools: The human factor. Educ. Plan. 2020, 27, 23–39. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1252710&site=eds-live&scope=site (accessed on 2 February 2021).
20. Patrascu, P. Promoting cybersecurity culture through education. eLearning Softw. Educ. 2019, 2, 273–279.
21. Bayard, E.E. The rise of cybercrime and the need for state cybersecurity regulations. Rutgers Comput. Technol. Law J. 2019, 45, 69–96. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=egs&AN=144292728&site=eds-live&scope=site (accessed on 2 February 2021).
22. Bhatnagar, N.; Pry, M. Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. Inf. Syst. Educ. J. 2020, 18, 48–58. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1246231&site=eds-live&scope=site (accessed on 12 February 2021).
23. Tang-Mui, J.; Chan-Eang, T. Impacts of social media (Facebook) on human communication and relationships: A view on behavioral change and social unity. Int. J. Knowl. Content Dev. Technol. 2017, 7, 27–50.
24. Nyblom, P.; Wangen, G.; Gkioulos, V. Risk perceptions on social media use in Norway. Future Internet 2020, 12, 211. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=147738607&site=eds-live&scope=site (accessed on 12 February 2021).
25. Atiso, K.; Kammer, J. User beware: Determining vulnerability in social media platforms for users in Ghana. Libr. Philos. Pract. 2018, 1–25. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=lxh&AN=133873708&site=eds-live&scope=site (accessed on 14 February 2021).
26. Pensa, R.G.; Di Blasi, G. A privacy self-assessment framework for online social networks. Expert Syst. Appl. 2017, 86, 18–31.
27. McCormac, A.; Zwaans, T.; Parsons, K.; Calic, D.; Butavicius, M.; Pattinson, M. Individual differences and Information Security Awareness. Comput. Hum. Behav. 2017, 69, 151–156.

28. Cain, A.A.; Edwards, M.E.; Still, J.D. An exploratory study of cyber hygiene behaviors and knowledge. J. Inf. Secur. Appl. 2018, 42, 36–45.
29. Ogutcu, G.; Testik, O.M.; Chouseinoglou, O. Analysis of personal information security behavior and awareness. Comput. Secur. 2016, 56, 83–93.
30. Nalaka, S.; Diunugala, H. Factors associating with social media related crime victimization: Evidence from the undergraduates at a public university in Sri Lanka. Int. J. Cyber Criminol. 2020, 14, 174–184. Available online: http://wintec.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edo&AN=143029465&site=eds-live&scope=site (accessed on 6 February 2021).
31. Schilder, J.; Brusselaers, M.; Bogaerts, S. The Effectiveness of an intervention to promote awareness and reduce online risk behavior in early adolescence. J. Youth Adolesc. 2016, 45, 286–300.
32. Furnell, S.; Khern-am-nuai, W.; Esmael, R.; Yang, W.; Li, N. Enhancing security behaviour by supporting the user. Comput. Secur. 2018, 75, 1–9.
33. Torten, R.; Reaiche, C.; Boyle, S. The impact of security awareness on information technology professionals' behavior. Comput. Secur. 2018, 79, 68–79.
34. Chang, L.Y.C.; Coppel, N. Building cyber security awareness in a developing country: Lessons from Myanmar. Comput. Secur. 2020, 97, 101959.
35. Muniandy, L.; Muniandy, B.; Samsudin, Z. Cyber security behaviour among higher education students in Malaysia. J. Inf. Assur. Cyber Secur. 2017, 2017, 1–13.