Information Security Assessment Among Teenagers

Radhakrishnan. Satish[1], Rajendran. Lavanya[2], and Devi. Lakshmi[3]
[1,2,3] Department of Media Sciences, Anna University Chennai

***Abstract*—The quantity of information transmitted between users has undergone an unprecedented change due to the introduction of digital communications. However, as the use of the internet has increased, so have the risks that come along with it. The users are typically the weakest link in the security chain; therefore, raising their awareness of information security has become a cornerstone for increasing vigilance among them. The ability of organizations and the general public to handle sensitive data is threatened by attacks like social engineering and phishing. The victims of the data loss could suffer irreversible psychological, monetary, and even material losses. Through pre- and post-test analyses, this study attempted to determine the efficacy of the security training, particularly about phishing, and to comprehend the user's attitude toward security practices. The study revealed marginal security awareness among college students. However, effective video and text-based training reversed and enhanced security practices.**

***Index Terms*—Information Security, New Media, Social Media, Teenagers.**

I. INTRODUCTION

The speed and volume of data transfers between people and groups have changed with the advent of information technology. Technology has made it easier to communicate for both personal and professional goals in this digital age. A platform for education, communication, entertainment, and information has been created by the internet and the emergence of social networks through Web 2.0 (Ratheeswari, 2018). It is now feasible to reach any corner of the world within a second thanks to the widespread use of mobile phones and the spread of the Internet to many sectors of society (Zhang, 2017). The advent of Web 2.0 made changes to how people pay their bills, shop for food and spend their free time. Many sectors and industries received technical adoption as a result of this achievement and growth (Adam & Alhassan, 2021). Trillions of bytes of data are exchanged electronically every second. The explosive rise of online social networking sites over the past ten years has dramatically changed the volume and nature of information transmission. Due to the students' extensive data transactions and associated vulnerabilities, there has been an increase in cybercrime, and they have been the target of online fraud. Numerous academic institutions have taken note of recent occurrences and have undertaken a series of measures to raise students' knowledge of information security. Numerous studies have been conducted to look into the knowledge gap regarding information security and how it relates to user awareness (Ramalingam et al., 2016), and in most cases, the users were considered its weakest link (Ganesh et al., 2022).

II. INFORMATION SECURITY

Teaching users about cyber security is more important than ever as Internet usage and social media usage grow. Even when consumers are aware of the risk posed by cyberspace, they frequently neglect to take the necessary preventative measures. Even though they are aware of this, they often fail to include preventative measures in their daily practices even though they are simple to implement (Zwilling et al., 2020). The utilization and sharing of information records are significantly influenced by how important self-efficacy and capacity threats are seen to be (Hooper & Blunt, 2020). Due to consumers' propensity to proportionately disclose even private information online, security concerns have grown (Henson et al., 2011). Students can connect because of the availability of inexpensive mobile devices and internet connections. This quickens the development of enormous amounts of personal and academic data, opening the door for cyberattacks. The lack of associated behavior and their understanding of safety procedures coincide with an increase in their threat (Moletsane & Tsibolane, 2020).

III. METHODOLOGY

The quantitative survey methodology based on the questionnaire was circulated to the college students. Prior permission was received from the respondents, and only the consenting students were allowed to participate in the study. All the respondents were over eighteen years old. Finally, 36 students participated in the pre-test, with equal numbers of men and women. This was followed by security training based on the material issued by the government and circulated to the students. Later, a video-based tutorial was screened and explained in detail about the security practices. The respondents were assessed on passwords and phishing. The distinction between the strong and weak passwords was tested through objective-type questions like asking the users to select the strongest password among sr24#ksn, foodie01, india123, and querty007. Similarly, in a case study-based question, for instance, the respondent was told that they received a call from an unknown user. The caller introduces her as college staff and asks to share your personal information. These case study-based questions were asked to evaluate the student's understanding of phishing.

IV. RESULTS

The student's responses were recorded through a Google Form and analyzed further for descriptive statistics. The students tend to use the internet through various electronic devices, but predominantly from their mobile phones (100%). In addition to this, around 41% of the respondents use their laptops (41.7%) to access the internet. 8.3% of students also use tablets and personal computers (8.3%), along with their phones, for internet usage. The majority of respondents (64%) spend more than 4 hours every day on the internet, revealing that it is an essential part of their daily lives. Around 18% of students spend 2-3 hours every day, and 9% spend 3–4 hours. Another 9% use it for 1-2 hours.

The respondents enquired about their internet usage purposes. The result revealed that using social networking sites (91.7%) was the dominant factor in internet usage. Checking emails (66.7%) and for educational purposes (66.7%) were next in line to the social networks. Information seeking (58.3%), online shopping, and games (41.7%) were in decreasing order of preference among students.

The vocabulary test is considered a standard practice to evaluate information security awareness. The security terms were asked to evaluate the students' awareness of them. The result of this terminology assessment revealed a low level of security understanding among the students. Phishing, cyberstalking, and sexting received a poorer response than hacking, online harassment, and malware. The female students scored below the males in almost all except harassment. Phishing refers to deceptive emails or webpages that lure the victims to share sensitive information, thereby causing financial and psychological troubles for the users. Sexting is the act of sending sexually explicit content to users.

Malware is an intrusive application that damages electronic systems to gain unauthorized access to their information or interfere with their security parameters to leak data to third-party networks. The female students scored 1.16, whereas the male students recorded 1.5 with respect to phishing. The female students notched 3.50, whereas male students recorded 3.22 with respect to online harassment. The female students scored 1.27, whereas the male students slashed 1.77 with respect to cyberstalking. The female students scored 2.05, whereas the male students scored 2.88 with respect to malware. The female students scored 1.0, whereas the male students scored 1.5 with respect to sexting. The female students recorded 3.0, whereas the male students scored 3.16 with respect to hacking. The female students logged 1.38, whereas male students scored 1.83 with respect to revenge porn. The female students scored 1.66, whereas the male students notched 1.94 with respect to social engineering.

Spam mail is a breeding ground for phishing. The curiosity and the quest for offers, discounts, and attractive messages make the users fall prey to fraudsters. The malicious codes and links attached to the emails compromise the electronic devices and can steal the sensitive data stored on them or track each user's actions without their knowledge. The emails from unknown sources carry the threat of carrying malicious attachments. The phishing technique includes receiving emails that look like those from known sources and misleading the users to click the links or redirecting them to enter sensitive information. The questions were listed on a five-point Likert scale, with 1, 2, 3, 4, and 5 corresponding to never, rarely, sometimes, often, and always, respectively.

The best way to prevent intrusion by invaders through emails is by deleting anonymous emails. The respondents here, with more than 70%, tend to open these kinds of emails. Spam mail is a breeding ground for phishing. Yet the students check the mail content. Approximately a quarter of the students do it at least once in a while. The most popular way of luring users and phishing them is through attractive offers and discounts. This makes the users lean towards the offers to check them out further. The 8% of students who always open the mail for discounts. Online games are a popular feature on the internet. Phishing emails tend to send links for playing famous games. Once clicked, it would be redirected to an unsecured webpage or malware would be downloaded into their system. 44% of students practice this sometimes.

The passwords are the first layer of protection for the online resources. This authenticating tool acts as a gateway to the accounts and needs to be regularly changed at intervals of thirty days. Strong passwords with a combination of alphanumeric characters and symbols make them difficult for hackers to crack easily. It could be password-, fingerprint-, or iris-protected, or even voice-based. Here, none of the students practice this trait on an all-time basis for all their devices. The majority of students use protective measures like lock screens. As mentioned earlier, alphanumeric passwords provide a higher level of protection than alphabet-based passwords. However, only 13% of students practice this password combination often. The passwords must be changed regularly, and the users must use different combinations for every account. Only 2.7% of students change their passwords regularly.

The students were required to undertake an assessment based on the online security training. They secured an average score of 14.4 points out of 20 in the post-training assessment. The range varies between 7 and 20, with a median score of 14. The students did better at distinguishing strong passwords from weak passwords. The respondents performed on an average scale in the case-based questions.

The vocabulary test after the training revealed a significant increase in the students' understanding of cybersecurity terminologies. The students performed better in all the terminologies. In the pre-test, they scored 1.33, and in the post-test, they scored 4.1 for phishing. In the pre-test, they recorded 3.36, and in the post-test, they scored 4.7 for online harassment. In the pre-test, they scored 1.52, and in the post-test, they notched 4.27 for cyberstalking. In the pre-test, they recorded 2.47, and in the post-test, they scored 4 for malware. In the pre-test, they scored 1.25, and in the post-test, they scored 4.5 for sexting. In the pre-test, they notched 3.08, and in the post-test, they scored 4.69 for hacking. In the pre-test, they scored 1.61, and in the post-test, they recorded 4.38 for revenge porn. In the pre-test, they counted 1.80, and in the post-test, they scored 4.19 for doxing.

V. CONCLUSION

Information security has become an essential aspect of cyberspace due to the increase in digital communications. This drastic growth in data exchanges has turned the pointer towards data vigilance and security awareness. With ever-increasing security breaches and financial exploitation by criminals of vulnerable users, the scope for user training has increased. As the weakest point in cyberspace, the users have become the most susceptible link in the security parameters for the organization to cope with the anti-social elements trying to lure potential users with social engineering techniques. This study, through the pre-test, tried to understand the level of security practices as well as the attitude of college students toward information security.

The results revealed a low level of security knowledge and practices among the students. Further intervention through security training was undertaken through text-based and video-based tools. The post-test assessment revealed a drastic increase in their security awareness and a substantive increase in their practices. Especially the scores concerning their passwords and phishing practices revealed the success of the training materials as well as the improvement in their behavior. As the cyber world has become an inevitable part of the current generation's actions, it is extremely important to inculcate and nurture security knowledge to remain vigilant and prevent digital crimes.

REFERENCES

[1] Adam, I. O., & Alhassan, M. D. (2021). The effect of mobile phone penetration on the quality of life. Telecommunications Policy, 45(4), 102109.

[2] Ganesh, A., Ndulue, C., & Orji, R. (2022, March). Smartphone security and privacy–a gamified persuasive approach with protection motivation theory. In International Conference on Persuasive Technology (pp. 89-100). Cham: Springer International Publishing.

[3] Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. Criminal Justice Review, 36(3), 253-268.

[4] Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. Behaviour & Information Technology, 39(8), 862-874.

[5] Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

[6] Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. arXiv preprint arXiv:1602.06510.

[7] Ratheeswari, K. (2018). Information communication technology in education. Journal of Applied and Advanced Research, 3(1), 45-47.

[8] Zhang, X. (2017). Exploring the patterns and determinants of the global mobile divide. Telematics and Informatics, 34(1), 438-449.

[9] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. Journal of Computer Information Systems, 1-16.