Journal of Advanced Research in Social Sciences and Humanities
Volume 8, Issue 2 (59-68)
DOI: https://dx.doi.org/10.26500/JARSSH-08-2023-0202

Importance of Conducting Cyber Security Awareness Sessions among Undergraduate Students

Arshiya Subhani [1]*, Iftikhar Alam Khan[2] , Usman Ahmad[3]
[1,2,3] Bath Spa University Academic Center, Ras Al-Khaimah, UAE

Abstract

Aim: In this digital era, a person's day begins with digital devices such as digital watches or smartphones. Cyber security is one of the major concerns in this era. Every device is connected, and hence, it is one of the reasons for most of the data security issues. The aim of this paper is to find out if it is necessary to conduct cybersecurity awareness sessions among students of different fields of study.
Methodology: To answer this question, a survey is conducted using the questionnaires and respondents are students from three different fields of study: Creative Computing, Business and Management and Psychology at BSU Academic Center, RAK, UAE. The data collected from 141 respondents was well analyzed.
Findings: : The findings show a significant difference between the responses of three fields of study. The students of Creative computing are well aware of cyber security terminologies compared to students from other fields of study.
Implications/Novel Contribution: The students can be guided with appropriate cyber laws to understand the importance of data security. In the future, cyber security awareness could be created among students by conducting seminars and workshops.

Keywords: Cyber security, Cyber threats, Cyber security awareness, Credential sharing, Unauthorized access

Received: 11 January 2023 / **Accepted:** 19 April 2023 / **Published:** 19 June 2023

INTRODUCTION

Cyber Security is one of the most important factors in this Digital era. Since 2020, there has been tremendous growth in the usage of electronic devices. As per the statista report Statista (2022), there are more than 5 million internet users, which is approximately 63.1 % of the total world population. After the pandemic 2019, most of the tasks are accomplished digitally, and every sector is dependent on technology. The benefits of this new trend in technology range from providing instant access to data on the cloud to the more advanced automation-based services using IoT. Every new trend has some potential threats and could lead to great loss if you are unaware of its consequences. Cybercrimes are increasing rapidly, and this is one of the reasons to have a basic knowledge of Cybersecurity. The term cyber-attack is heard every other day in the media. Due to the rapid rise of electronic device usage in most of the sectors like Healthcare, Education, Industry, Farming, and many more, and with the advancement of IoT in most of the sectors, there is a huge risk of creating a target-rich environment for hackers and the cyber threats are always close at hand. The study by NortonLifeLock (2022) found that 72% of parents of children under 18 say their children have used their mobile devices without their permission. The study also revealed that 27% of children clicked suspicious links, 24% of children shared their personal information, and 25% of children viewed mature content. It is more important now than before to create cyber security awareness in children.

What is Cyber Security?

The author in Sheth, Bhosale, Kurupkar, and Prof (2021), "It could be defined as the procedure to ease the security fears to protect repute damage, commercial loss or financial loss of all groups." Generally, it is the process of protecting the devices from digital attacks. These cyber-attacks are usually aimed at assessing, changing, or

*Corresponding author: Arshiya Subhani
†Email: arshiya@bathspa.ae

destroying sensitive information; extorting money from users via ransomware; or interrupting normal business processes". Cyber security awareness is important because it provides security to different data types and devices connected via some network. Security here doesn't mean providing security only to the connected devices but also securing the associated data. There are different types of attacks, such as physical and nonphysical attacks. The physical attacks damage physical devices such as applications, servers, systems, printers, routers, etc. The nonphysical attack uses some software or illegitimate codes and affects the devices' software.

In the large business world, many organizations perform daily tasks digitally, like online meetings using video conferencing, sharing data digitally, storing data in the cloud like Google Drive, and many more. Securing all of this information is most important. Providing security is not only the job of the IT Security officer, but everyone connected to the network should be concerned about it. In most cases, it is not always the attacker who hacks; the attack could be due to the negligent behavior of the employee. Hence, all employees should be aware of the basic terminology associated with cyber security. Educating the young generation is a great step towards successfully implementing the security features.

Cyber Security Threats

Threats are classified as natural threats, human threats, and technical/cyber security threats. Natural threats are the ones that occur naturally, like earthquakes, hurricanes, tsunamis, and many more. The human threats are the ones that occur due to human behavior and affect the environment, like global warming, Pollution, and many more. On the other hand, technical threats are the ones that affect the hardware and software of the various devices. Cyber security threat is a malicious act that seeks to damage or steal data and disrupt digital life in general. Cybersecurity threats describe the activities of cyber criminals and the different methods of implementing malicious attacks.

Cybercriminals use different types of malicious cyber threats. Some of them are described in Figure 1. The impact of these threats is significant to the organizations. Every organization should have countermeasures to protect from these threats.

Malware attacks are generally malicious software that can harm the computer and data stored in it using the malicious code. In 2020, 700 million new malware will emerge and attack billions of electronic devices Rohith and Kaur (2021). Some examples of Malware attacks are ransomware, Viruses, worms, Trojan Horse, etc. When a malicious intruder intercepts the communication channel by just monitoring the communication, it is called a Man-in-the-middle attack. This type of attack aims to gain user information such as login credentials, credit card numbers, account details, mobile numbers, email IDs, etc. Social Engineering attacks directly involve humans by creating urgency, fear, or any similar behavior that causes them to click a link or open a particular file. Social engineering attacks include Phishing, Baiting, Vishing, Pretexting, Piggybacking, etc. Denial of service attacks are used to provide a certain service unavailable for a certain amount of time using methods such as HTTP flooding, SYN Flooding, TCP Flooding, UDP flooding, etc. Supply chain attacks are also called third-party attacks or value chain attacks; these types of attacks occur when an outsider enters your system through the outsider who has your system access. Some examples of supply chain attacks are compromising on building tools or developer accounts, installing malicious code into automated updates, etc. Injection Attacks occur when the intruder injects some malicious input into the program code, which alters the program output and gives unexpected results. Examples of injection attacks are SQL injection, Code injection, OS command injection, etc.

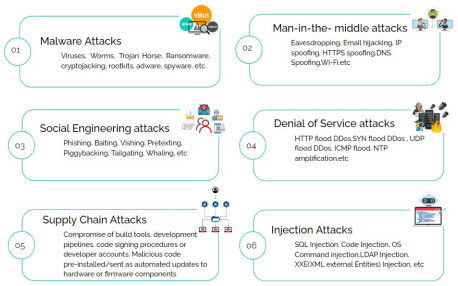

Figure 1. Different types of Cyber Security Threats

Protection from these cyber security threats is one of the major concerns in today's business world. Many organizations follow security mechanisms to prevent these threats.

Need of Cyber Security Awareness Among Children

These days, the Internet is widely used by people worldwide to share ideas, messages, discussions, opinions, and express their feelings. Many social media platforms like Facebook, Instagram, Twitter, YouTube, and TikTok enroll users for free of cost and use the platform to perform various activities such as enhancing their popularity, sharing feelings, daily activities and responding to public messages Pencheva, Hallett, and Rashid (2020). The Internet is a borderless virtual environment that connects about 2.7 billion people. The Internet offers, on the one hand, vast numbers of benefits, and on the other hand, it also provides equal opportunities for cyber-terrorists and hackers (Goutam, 2015). In this digital era where, the Internet is available to all people, including children, youth, and adults. So, it is mandatory for youngsters to acquire knowledge and education on cyber security to create a habit of using the Internet following all security mechanisms (Amankwa, 2021).

Youngsters are efficient in using the Internet and digital devices, especially smartphones, which consist of many applications. It becomes difficult for parents to monitor their children's internet activities, which is one of the primary reasons for the tremendous increase in cyberbullying among children. As per the study on children's internet usage Martin (2015), most children spend time watching cartoons, animated movies, and listening to songs. As usage of the Internet by Children is increasing daily, it is important for them to understand the threats associated with it. Knowledge of cybersecurity will protect children from becoming victims of cybercrime. It is the responsibility of educators to promote cyber security awareness among children to protect them from various cyber threats (Trappe & Straub, 2018). Educators can also involve parents in creating cyber security awareness among children. According to previous research, children who use the internet more and spend most of their time playing games and watching cartoons or movies online develop antisocial and aggressive behaviors. Children are susceptible, and some of them with low self-esteem are easily affected by hateful comments (Trappe & Straub, 2018). Considering all of these things, it is crucial to educate these youngsters on cybersecurity concerns to protect them from being victims of cyber attacks.

LITERATURE REVIEW

Educating children about cyber security and its issues at different levels of education is required to create awareness of the threats and impact of cyber-attacks. As per the cyber security body of knowledge Rashid et al. (2018), cyber security is one of the essential elements to be added to curricula at all education levels.

The ConRed program was conducted to prevent cyberbullying involving students, teachers, and families. Eight sessions were conducted over a duration of 3 months, and the results showed that there was a reduction in cyberbullying and cyber victims (Del Rey, Casas, & Ortega, 2016). This proves that conducting awareness sessions can have a good impact on the reduction of cyberbullying. An information security survey was conducted in Los Angeles in the College of Business and Economics at California State (Slusky & Partow-Navid, 2012). As per the survey results, most of the security issues are due to the poor implementation of security knowledge in real-time problems. The study related to ISA in Ahlan, Lubis, and Lubis (2015) stated that security awareness is also dependent on religious factors and influences individual performance and social pressure. The other study in Kuwait universities Al-Alawi, Al-Kandari, and Abdel-Razek (2016) identified knowledge, attitude, and behavior as the factors affecting information security awareness and also stated the s six focus areas to enhance awareness in higher education. The results from the study, which focused on investigating student awareness and behavior in cyber security in California Silicon Valley, states that even though the students were aware that the information shared on the internet is monitored in the university systems, they were unaware to follow the procedures to protect their data (Moallem, 2019). In the other study Taha and Dahabiyeh (2021), where an empirical comparison is made between computer and smartphone usage and its related security issues, states that even though students were aware of the cyber security issues, they didn't follow the security mechanisms to protect their data in smartphone compared to computers, hence suggested to provide training campaigns to educate students on the security risks and concerns of data in smartphones.

In Nigerian universities, the study Alharbi (2022) focused on the student's enthusiasm to learn cyber

security and its awareness by surveying to find out if the students in the developing country were aware of the attacks and their consequences and whether cyber security awareness programs are part of University programs. The findings revealed that the students were aware of cybersecurity but didn't know how to protect their data. Most of the universities have no cyber security awareness as a part of the programs; however, students showed interest in learning cybersecurity concepts. The information security awareness study Aloul (2012) in UAE among students and other professionals suggested the importance of controlled audits and other factors to enhance security awareness among individuals. The study at Yobe University Garba, Siraj, Othman, and Musa (2020) investigated security awareness among students in the computer science department and found that half of the students were unaware of how to protect their data and hence suggested a cyber-security awareness program. Another study at Majmaah University, KSA Alharbi and Tassaddiq (2021), stated that there is a need to educate and train the students in cyber security awareness programs. A survey on security threats was conducted in Tamil Nadu, and the findings revealed that college students had above-average levels of cybersecurity awareness (Aliyu, Abdallah, Lasisi, Diyar, & Zeki, 2010). The survey was based on cyber-attacks related to email, phishing, popup windows, fake advertisements, etc. The other study in Senthilkumar and Easwaramoorthy (2017), a private tertiary education system in South Africa, conducted a survey focusing on cyber security knowledge, self-perception of cyber security skills, actual cyber security skills and behavior, and cyber security attitudes. The findings revealed that cyber security campaigns are necessary to address cyber security issues. As per the study in Chandarman and Van Niekerk (2017) revealed that 23% of South African users change their passwords regularly; however, 70% of the users were aware that changing passwords is a good practice. Based on the research conducted Alqahtani (2022) among the students of Imam Abdulrahman Bin Faisal University College in KSA, their knowledge of passwords, browsers, and social media security issues revealed that these factors influence cybersecurity awareness among students. The above studies state that there is an urgent need for cyber security awareness programs among students, which help to protect their personal data from cyber-attacks by following very basic security mechanisms.

METHODOLOGY

The research conducted is based on the quantitative method using the survey with a set of questionnaires. The primary purpose of the research is to answer the Research question - Is it necessary to conduct cyber security awareness sessions for students of various fields of study at Bath Spa University RAK Campus?

This section describes the methodologies used to gather the data for conducting research to answer the stated research question. A survey was conducted using questionnaires. The questionnaire was organized to obtain cyber security awareness among undergraduate students belonging to three different fields, such as Creative Computing, Business & Management, and Psychology at Bath Spa University Academic Center RAK. The questionnaire has 16 questions to make it easy for students to complete in less than 5 minutes, primarily by selecting yes/no options.

The questionnaire follows the standard questionnaire set used by researchers in their study to obtain cyber security awareness in higher education (Garba et al., 2020) . The survey was conducted by sharing the questionnaire with students using Google Forms. For current research, the Google form was used to conduct a survey and shared via WhatsApp group messages to all students. There were a total of 141 respondents. The insights from the survey were conducted for the student's age group of 17 - 21.

DATA ANALYSIS AND FINDINGS

The data collected is analyzed using different methods like cross-tabulation. The data is analyzed based on gender and Field of study. The data analysis process is described using the charts.

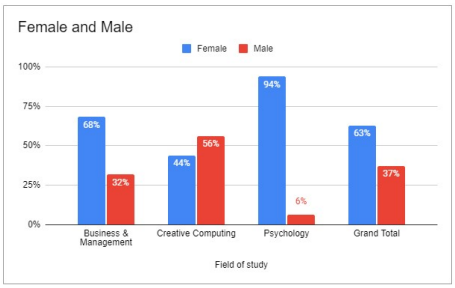

Figure 2. Male and Female Respondents

Figure 2 above shows the total male and female respondents for three different departments. Of the total respondents, 63% were female and 37% were male.

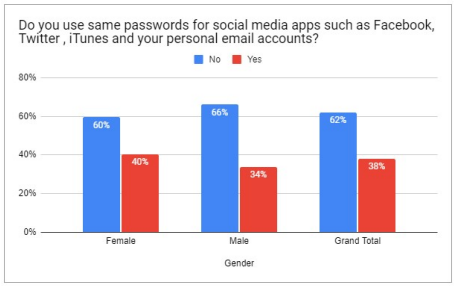

Figure 3. Using the Same Passwords

The above figure 3 shows that among 41% of female students and 34% of male students use the same passwords. In total, 38.46% of students were using the same password. There is a high risk of compromising passwords if the same passwords are used in different locations. The figure also shows that the percentage of female yes respondents (41%) percentage is more than that of male yes respondents (34%).

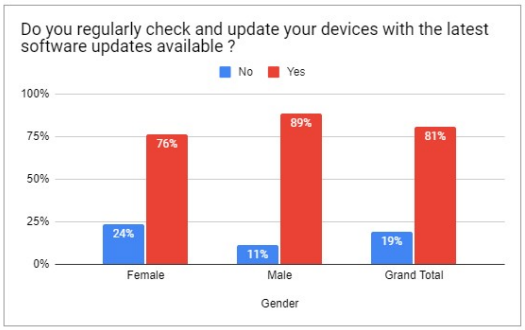

Figure 4. Check and Update Devices

Software updates are frequently available, and sometimes people avoid updating software, which could lead to cyber-attacks. Generally, updates fix the bugs or loopholes in the software. Outdated software is more vulnerable to cyber-attacks as cybercriminals would be aware of the exploitable holes in the software to perform the attack on the devices. Figure 4 above shows that about 81% of students frequently update their devices with the latest updates. 19% of students are unaware of the importance of updating the software on their devices.

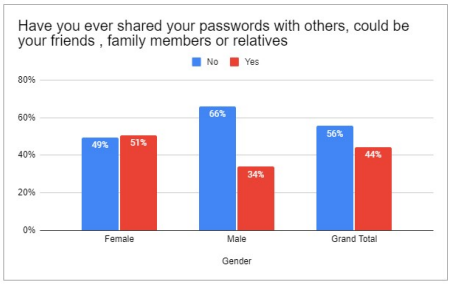

Figure 5. Sharing P]asswords

Sharing passwords with family and friends would sometimes be very risky. There are many disadvantages to sharing passwords. The first and foremost risk is that the accounts/devices would be compromised and no longer be secure. Sharing passwords can be one of the reasons for the accounts/devices to be more vulnerable to phishing attacks. Figure 5 shows that 44% of the students shared their password with others.

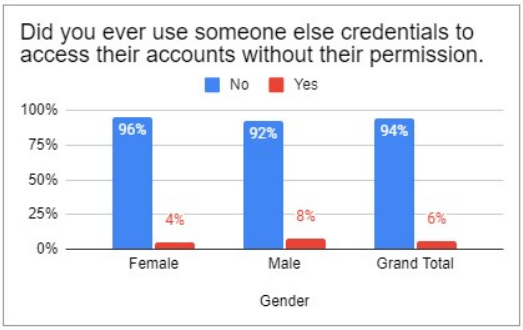

Figure 6. Unauthorized access

Everyone has accounts these days for almost every application they use. Logging into someone else's account without their permission is illegal. Nowadays, students are completely aware of the importance of credentials. As per the survey results, only 6% of students used someone else credentials without their permission, as shown in Figure 6.

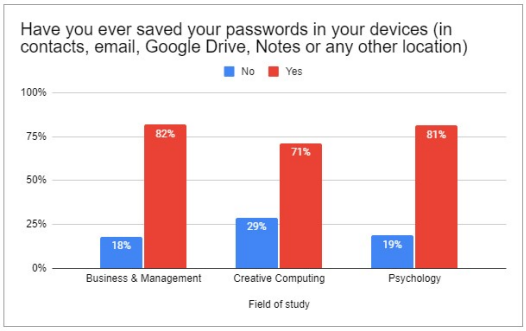

Figure 7. Saving Passwords in Devices

Every application requires authorized users to log in using their login credentials. It is always advised to have different passwords for different sources. Most people find it challenging to memorize passwords and hence store the credential details like passwords in devices at different locations such as in emails, Google Drive documents, contacts section, notes, etc. As per the findings, 77% of students store passwords on their devices. It is essential for them to understand the importance of maintaining secrecy about their credentials. Students need to know that if a password is compromised, then unauthorized users can access their data either maliciously or

unintentionally.

The above graph in Figure 7 shows that the percentage of Business management and psychology students who save passwords on their devices is above 80%, which is higher than that of the Creative computing respondents, which is 71%. This figure clearly shows that business management and psychology students are not aware of the risks involved in storing passwords on their devices.

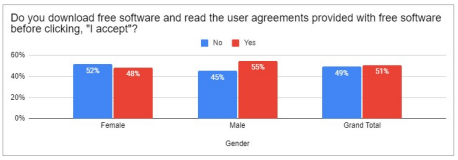

Figure 8. Read the Terms and Conditions

A myth about downloading software is that it is not required to read the agreement before clicking the "I agree" button. As per the findings in Figure 8, 51% of the students are not aware of the importance of reading the user agreements while downloading the software before clicking; I accept.

Most of the students use social media websites such as Facebook but are unaware of the terms they agree on. For example, Facebook stores your data whether you have an account or not; The service can read your private messages and history and Delete (Wikipedia, 2012). Unaware of these permissions granted, all users share their personal information on social media sites. Creating awareness about the importance of reading the terms is most important to students.

Private information can be secured by hiding it from others. Logging out from the devices/accounts with private information secures the data and reduces the risk of data leakage. As per the findings, as shown in Figure 9, 15% of students sometimes forget to log out, and it is understood that 85% of students are aware that it is not always possible to log out remotely from all accounts, for example, in email accounts. The best way to protect our accounts if we forget to log out from public devices is to reset the password.

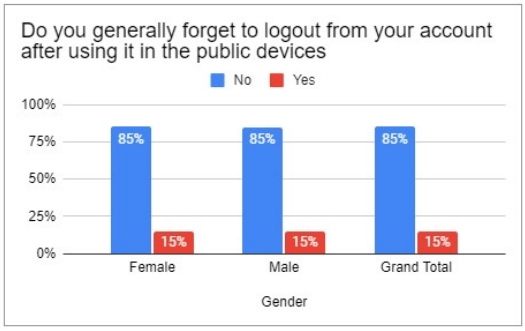

Figure 9. Forget to Logout

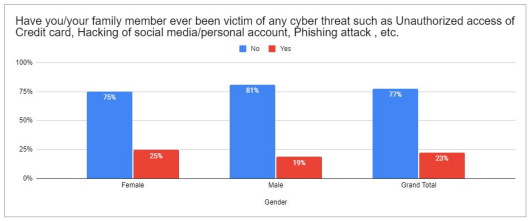

Figure 10. Victim

Generally, people could be cyber victims if they are unaware of cyber threats like phishing, spamming, hacking, unauthorized access to accounts, etc. Most of the students are aware of these terms, and the findings, as

shown in Figure 10, state that only 23% of respondents were cyber victims. Most positive respondents were victims of unauthorized access to their social media accounts and credit cards. Even though no significant manipulation was reported, it was still discovered that hackers consider even students to be their victims.

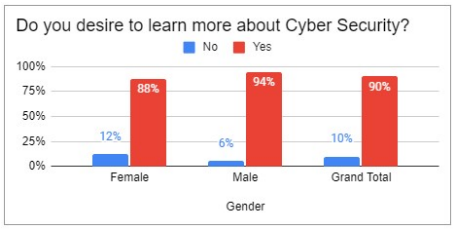

Figure 11. Desire to Learn Cyber Security

Most of the students are interested in learning the concepts of Cybersecurity. As per the survey findings, as shown in Figure 11, 90% of students are interested in learning more about cyber security. These young students are always active on their digital devices, either for their education tasks or for fun. Most of the students always find it difficult to understand the security terminologies, and hence, they are eager to learn the concepts of cyber security.

Findings Based on Field of Study

The following responses to the questions are represented in the figure below.

- Do you regularly check and update your devices with the latest software updates available
- Did you ever use someone else credentials to access their accounts without their permission?
- Do you download free software and read the user agreements provided with free software before clicking "I accept"?
- Do you generally forget to logout from your account after using it on public devices?
- Have you/your family member ever been the victim of any cyber threat such as Unauthorized access to Credit cards, Hacking of social media/personal accounts, Phishing attacks, etc?

The graph clearly shows that Creative computing students know the consequences of ignorance of cyber security issues. The Business & Management and Psychology department respondents need further knowledge on the cyber security issues and control mechanisms. For instance, consider the question, "Have you ever shared your password with others, could be your friends, family members, or relatives?" 32% of creative computing students responded yes, which is less than the Business & Management and Psychology respondents, which is 52% and 59%, respectively.

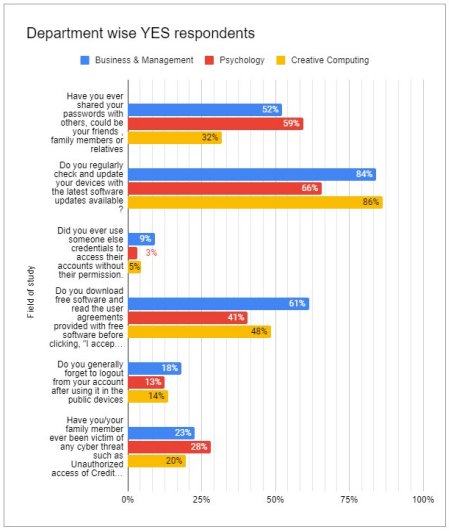

Figure 12. Yes Respondents For the Survey Questions Based on the Field of Study

CONCLUSION

The main aim of this paper was to conduct a questionnaire-based survey to analyze their understanding and awareness of cyber security concepts. This digital era brings a lot of security concerns, which are to be addressed at the very first step. Most of the students have more than one digital device. Providing data security and authorized access to the devices is much more important. The questionnaire was designed to collect the information about students' knowledge of cybersecurity terminology. As per the findings, 90% of respondents are willing to learn about cybersecurity concepts. The students can be guided with appropriate cyber laws to understand the importance of data security. In the future, cyber security awareness could be created among students by conducting seminars and workshops.

Statement of Limitation

The limitation of this paper is that the number of respondents to the survey could be more. The respondents of the survey are only students; we could have also involved staff and faculty to understand the requirements to establish and implement the cyber security mechanisms at the campus. The various inferential statistics analyses could be used to support the null hypothesis.

REFERENCES

Ahlan, A. R., Lubis, M., & Lubis, A. R. (2015). Information security awareness at the knowledge-based institution: its antecedents and measures. *Procedia Computer Science*, *72*, 361-373.

Al-Alawi, A. I., Al-Kandari, S. M., & Abdel-Razek, R. H. (2016). Evaluation of information systems security awareness in higher education: An empirical study of kuwait university. *Journal of Innovation and Business Best Practice*, *2016*, 1-24.

Alharbi, T. (2022). Developing cost-effective cybersecurity management system for academic institutions in saudi arabia. *J. Eng. Appl. Sci*, *9*, 57.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of majmaah university. *Big Data and Cognitive Computing*, *5*(2), 23.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among iium students: An empirical study. In *Proceeding of the 3rd international conference on information and communication technology for the moslem world (ict4m) 2010* (p. A52-A56).

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, *12*(5), 2589.

Amankwa, E. (2021). Relevance of cybersecurity education at pedagogy levels in schools. *Journal of Information Security*, *12*(4), 233–249.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*, 133-155.

Del Rey, R., Casas, J. A., & Ortega, R. (2016). Impact of the conred program on different cyberbulling roles. *Aggressive behavior*, *42*(2), 123-135.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. (2020). A study on cybersecurity awareness among students in yobe state university, nigeria: A quantitative approach. *Int. J. Emerg. Technol*, *11*(5), 41-49.

Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications*, *111*(7).

Martin, K. M. (2015). Cyber security education, qualifications and training. *Engineering & Technology Reference*, *2015*, 8.

Moallem, A. (2019). Cyber security awareness among college students. In *Advances in human factors in cybersecurity: Proceedings of the ahfe 2018 international conference on human factors in cybersecurity, july 21-25, 2018, loews sapphire falls resort at universal studios, orlando, florida, usa 9* (p. 79-87).

NortonLifeLock. (2022). *Too trusting? over half of american parents let their kids go online without supervision.* Retrieved from https://shorturl.at/aoEG3

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68-74.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. *IEEE Security & Privacy*, *16*(3), 96-102.

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. In *2021 2nd international conference on intelligent engineering and management (iciem)* (p. 429-434).

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in tamil nadu. In *Iop conference series: Materials science and engineering* (Vol. 263, p. 042043).

Sheth, M. A., Bhosale, S., Kurupkar, F., & Prof, A. (2021). Reasearch paper on cybersecurity. *Contemporary research*, *2021SP*, 2231–2137.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26.

Statista. (2022). *Internet and social media users in the world 2022.* Retrieved from https://shorturl.at/bdjW5

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies*, *26*(2), 1721-1736.

Trappe, W., & Straub, J. (2018). Cybersecurity: A new open access journal. *Journal of Cybersecurity and Privacy*, *1*(1), 1-3.

Wikipedia. (2012). *Terms of service; didn't read.* Retrieved from https://shorturl.at/pruT2