IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12201

Cyber Security Awareness for Education Institutions

Alaa Ridha[1], Meshal AlDhamen[2]

Training Faculty, Computer Department, PAAET, Shuwaikh Education, Kuwait[1]

Training Faculty, Computer Department, PAAET, Shuwaikh Education, Kuwait[2]

Abstract: Cybersecurity is a critical issue for higher education institutions, as they store and manage a vast amount of sensitive data, including student records, research findings, and financial information. Higher education institutions are also increasingly reliant on technology for teaching, learning, and administration, which means that they are vulnerable to cyber threats such as hacking, phishing, and ransomware attacks. One of the key challenges in protecting higher education institutions from cyber threats is the fact that they often have complex and decentralized networks. This can make it difficult to implement and enforce consistent security measures across the entire organization. Additionally, higher education institutions often have many stakeholders, including students, faculty, staff, and external partners, which requires efforts to coordinate and manage information security.

Keywords: Cyber Security, Cyber security awareness, Information security.

I. INTRODUCTION

Like other businesses, universities and colleges are affected by the increase of cybersecurity crimes due to the wide range of services they offer online and the number of users accessing those services. Most higher education's institutions are offering Emails, Wi-Fi access along with different platforms for e-learning. According to Moallem (2019) 40% of college students from two universities in Silicon Valley, don't have enough knowledge or awareness of cybersecurity attacks. Moallam stated that 16% of students had no knowledge of any cybersecurity topics such as two-factor authentication, which means they are in higher risk of falling for cyber-attacks.

Students also reported that universities don't have the right programs to reach out students for improving their awareness about cyber-security attacks. According to a study by Kovacevic, Putnik, and Toskovic (2020) published by IEEE increasing student awareness on how to behave and protect themselves in the cyber space is the most significant factor in increasing cybersecurity awareness. This paper will discuss the major types of cyber-attacks on higher education institutions and best practices to design effective cybersecurity awareness programs.

II. TOP CYBER ATTACKS ON EDUCATION INSTITUTIONS

Recent article published in 2022 by the open-source government organization indicated that recent cyber-attacks on higher institutions had increased both in numbers and impacts. The article also claimed that some universities had to shut down services for a period that can sometimes last up to two weeks. The cost of a cyber-attack on a higher education institution can vary greatly depending on the severity and scope of the attack. However, it is estimated that the average cost of a data breach for a higher education institution is around $1 million.

This cost can include expenses related to investigating the breach, repairing the damage, and compensating affected individuals. Additionally, a cyber-attack can also result in lost business opportunities and a decline in reputation, which can lead to even greater costs in the long term. Ransomware had affected universities and caused to stop major services like online exams. According to Arthur (2021) the best way to prevent cyber-attacks is to educate students about the threats and risks related to cybercrimes. Mousa (2019) further explained the need to cybersecurity awareness campaigns due to the student lack of knowledge in topic like phishing and anti-virus software. The following list indicates the major cyber-attack types targeting higher institutions and best practices to prevent them:

A. Phishing

Phishing is the most common type of cyber-attacks targeting students and staff. These are emails that appear to come from a trustworthy source and try to trick the recipient into revealing sensitive information or downloading malware. Recent statistics showed an increase of 100% of phishing attacks in the last few years.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12201

Phishing attacks can take different forms like asking students to download copy of the lecture or bad links for cloud and e-learning services. This type of attack requires a training for both students and staff to distinguish the fake senders and be able to recognize phishing emails.

B. Malware

Malware defined as software that are designed to cause harm to systems or victims. This type of attack encrypts the victim's files and demands a ransom payment in exchange for the decryption key. Malware takes several forms including computer viruses, trojans, ransomware, or spyware. Universities and students around the world had fallen victims to hackers by accessing bad links. Therefore, services were severely interrupted and personal data such as passwords were stolen. The best way to stop malware is to educate students and staff about malware forms and what not to click. Malware usually is a human error that can be prevented by the right awareness programs.

Password Security
Weak passwords are easy to be hacked either physically or by program. Studies show that over 60% of people use the same passwords for different accounts, therefore passwords can be easily stolen. According to Alqahtani (2022) 30% of students in his study use one password for all websites. The best way to prevent this is by educating users about multi-factor authentication (MFA) to avoid breaking passwords. Higher institutions are also encouraged to use MFA for their services, especially emails.

C. DDoS Attack

A distributed denial-of-service (DoS) attack is another major type of attack in higher institutions. This type of attack happens when systems and servers are overflowed that they can no longer operate. The attack aims to disrupt the availability of a website or online service by overwhelming it with traffic. Hackers use a device on the network or system to install a malware before the attack begins. The best way to prevent this type of attack is by having the right plan, increasing security measures on networks, and using firewalls.

Other less frequent types of attacks can be the insider threats, which refers to individuals who have access to sensitive information and use it for malicious purposes, such as theft of data or intellectual property. Higher education initiations should also consider taking steps ahead against Advanced Persistent Threats (APTs), which are long-term, targeted attacks that are often carried out by nation-state actors. It is important for higher education institutions to implement strong cybersecurity measures and educate their staff and students about cyber threats to reduce their vulnerability to these attacks. Fig 1 summarizes the major types of attacks on higher institutions:

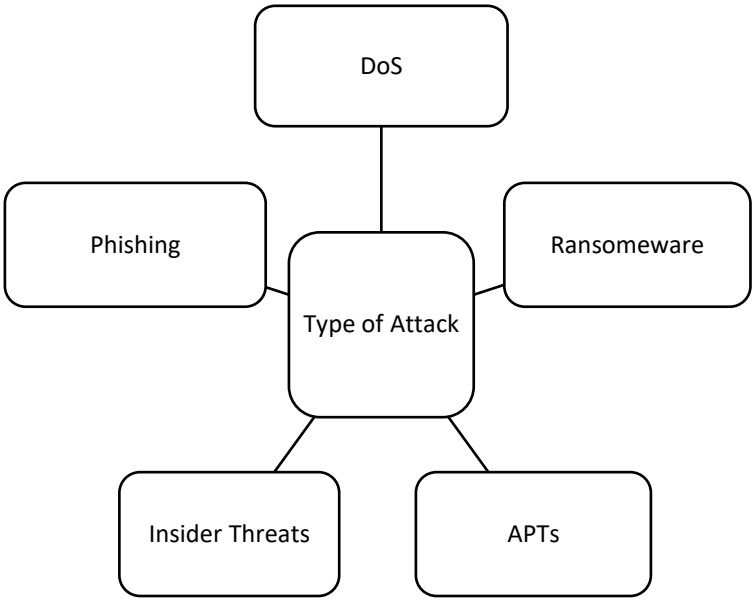

Fig. 1 Cyber security attacks

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12201

III. CYBER SECURITY PROGRAMS FOR HIGHER INSTITUTIONS

Many studies have showed the importance of cybercity awareness programs for college students. Alharbi and Tassaddiq (2021) indicated the following major components of cybersecurity awareness programs:

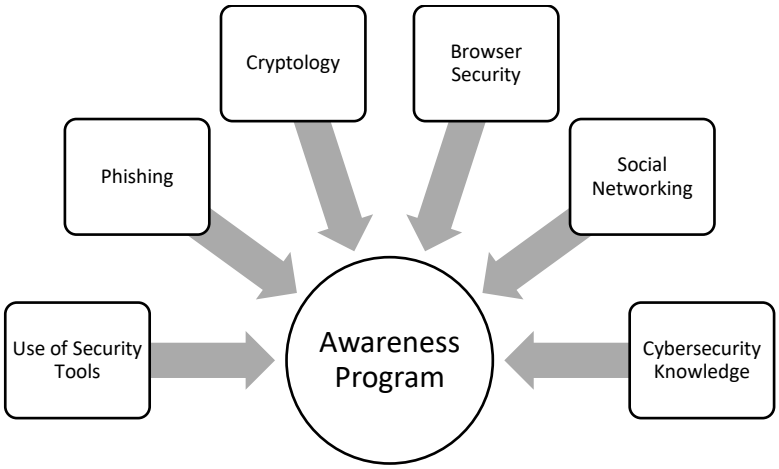

Fig. 2 Components of awareness programs

Other studies had also concluded the same positive impact of integrating the following elements in cybersecurity awareness campaigns; Alqahtani (2022) indicated 20.6% effect on students' cybersecurity awareness by empathizing the importance of using strong password, updating Internet browsers, and knowing how to behave in different social media platforms. According to Alharbi and Tassaddiq the best way to reach out students is combining different tools such as emails, presentations, newsletters, and SMS and using both text and videos.

According to Open Access Government article (2022) the cybersecurity awareness campaigns become a priority for higher education institutions. It also requires organizations to dedicate the appropriate budget and reaching out students and staff with the right training and updates.

The main goal of any awareness campaign is to make students and staff aware of cyber incidents, their risks and how to deal with them. It is very common to have the following standards when designing a cybersecurity awareness campaign, below are a list of main elements:

- Computer-based awareness training
- Phishing simulation exercises
- Awareness videos and posters
- In-person security awareness training
- Monthly newsletters for updates

In addition, the following steps can guide higher education institutions on designing an effective cybersecurity awareness program that helps to raise awareness and improve the security posture of the institution:

A. Identifying the target audience

The first step in designing a cybersecurity awareness program is to identify the target audience. This may include students, faculty, staff, and other stakeholders such as alumni, donors, and external partners.

B. Assessing the needs of the target audience

It is important to understand the needs of the target audience to design an effective awareness program. This may involve conducting surveys or focus groups to gather information about their knowledge, attitudes, and behaviours related to cybersecurity.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12201

C. Developing a plan

Based on the needs of the target audience, it is necessary to develop a plan for the awareness program. This may involve identifying specific goals and objectives, as well as the types of activities and resources that will be used to achieve those goals.

D. Implementing the program

Once the plan has been developed, it is important to implement the program in a way that is effective and engaging. This may involve using a variety of approaches, such as in-person training sessions, online resources, and interactive activities.

E. Evaluating the program

It is important to regularly evaluate the effectiveness of the awareness program to ensure that it is meeting its goals and objectives. This may involve collecting feedback from participants, as well as analysing data on the impact of the program.

Finally, it is very beneficial to combine different methods and practices when designing cyber security campaigns to reach out students and staff and achieve campaigns' goals. Here are some examples:

- Awareness campaign: Hold regular training sessions and workshops for students and staff to educate them about cyber threats and how to protect themselves. This could include topics such as phishing, strong passwords, and safe online behaviour.
- Phishing simulation: Conduct a phishing simulation to test the ability of staff and students to identify and respond to phishing attacks. This can help to raise awareness of the risk and improve their ability to detect and avoid phishing scams.
- Encourage strong passwords: Encourage students and staff to use strong and unique passwords and to use multi-factor authentication where possible. Regular password reminders can also be sent to encourage them to update their passwords regularly.
- Data backup and recovery plan: Develop and implement a comprehensive data backup and recovery plan to ensure that the institution is prepared in the event of a data breach or loss.
- Regular software updates: Regularly update all software and systems to ensure that they are protected against the latest threats.
- Network security: Implement strong network security measures such as firewalls, intrusion detection systems, and secure authentication methods to protect the institution's systems and data.
- Monitor for threats: Regularly monitor for threats and suspicious activity and respond quickly to any incidents. This can be done using security information and event management (SIEM) tools, threat intelligence feeds, and regular security audits.

IV. CONCLUSION

In conclusion, cybersecurity is a critical issue for higher education institutions, as they are vulnerable to cyber threats such as hacking, phishing, and ransomware attacks.

To effectively protect against these threats, higher education institutions must take a comprehensive and proactive approach, including developing and implementing a cybersecurity policy, providing training and education, implementing technical safeguards, enhancing physical security, and building partnerships with external organizations.

It is recommended that higher education institutions prioritize cybersecurity and allocate sufficient resources towards implementing and maintaining effective security measures. This may involve investing in technology, hiring specialized staff, and collaborating with external partners. By taking these steps, higher education institutions can significantly reduce their risk of cyber-attacks and protect their sensitive data and technology assets.

This, in turn, can help to maintain the trust and confidence of students, faculty, and other stakeholders, and to ensure the smooth operation of the institution.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12201

REFERENCES

[1]. A. Nassoura. “Cybersecurity Technologies And Practices In Higher Education Institutions: A Systematic Review,” Webology, vol. 19, pp. 1152-1167, Mar. 2022.
[2]. M. Alqahtani. “Factors Affecting Cybersecurity Awareness among Universities Students,” Applied Sciences, vol. 12, pp. 2589, Mar. 2022.
[3]. A. Kovačević, N. Putnik and O. Tošković, "Factors Related to Cyber Security Behavior," IEEE Access, vol. 8, pp. 125140 -125148, Jul. 2022.
[4]. A. Moallem, “Cyber Security Awareness Among college Students,” in Proc. AHFE, 2018, p. 79-87.
[5]. G. Arthur. (2021) Cyber Security in Universities: Identifying Risk, Threats, and Vulnerabilities. [Online]. Available: https://winbuzzer.com/2021/07/19/cyber-security-in-universities-identifying-risk-threats-and-vulnerabilities-xcxwgp/
[6]. Higher Education Cybersecurity: Protecting Institutions and Students. [Online]. Available: https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf
[7]. S. Campbell. (2022) Cybersecurity in Higher Education: Challenges and Strategies. [Online]. Available: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education
[8]. S. Mousa, “Cyber Security: Exploring Awarenss among University Students at a Public Educational Inistitutions,” IJIRK, vol. 4, pp. 88-97, May. 2019.
[9]. The benefits of cyber security awareness training within universities. [Online]. Available: https://www.openaccessgovernment.org/the-benefits-of-cyber-security-awareness-training-within-universities/139452/
[10]. T. Alharbi. A. Tassaddiq, “Assessment of cybersecurity awarenss among students of Majmaah University,” Big Data and Cognitive Computing, vol. 5, pp. 23-38, Jun. 2021.
[11]. E.C.K. Cheng, T. Wang, “Institutional Strategies for Cybersecurity in Higher Education Institutions,” Information, vol. 13, pp. 192, April. 2022.

 This work is licensed under a Creative Commons Attribution 4.0 International License