A Study on the Cyber Attack Awareness Among Students: University of Science and Technology Case Study

M. Khaled [1]
M. Saleh [1]
Y. Nasser [1]
F. Salah [1]
A. Hani [1]
M. Ahmed [1]
A. Abdullah [1]
A. Adell [1]
M. F. Abdullah [1*]
N. Alsakkaf [1]

Received: 23/03/2025
Revised: 17/07/2025
Accepted: 18/07/2025

[1] Faculty of Engineering & Computers, University of Science and Technology, Aden, Yemen.
*Corresponding Author's Email: m.albadwi@ust.edu , n.alsaqqaf@ust.edu

A Study on the Cyber Attack Awareness Among Student: University of Science and Technology Case Study

Mohammed Khaled
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohamed Saleh
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Youssef Nasser
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Firas Salah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Abdullah Hani
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohammed Ahmed
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Ali Abdullah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Abdullah Adell
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen

Mohammed Fadhl Abdullah
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen
m.albadwi@ust.edu

Nasr Alsakkaf
Faculty of Engineering & Computers, University of Science & Technology, Aden, Yemen
n.alsaqqaf@ust.edu

Abstract— This study addresses the significant risks faced by students at the University of Science and Technology (UST) – Aden Branch, stemming from the technological lag in Yemen and the sudden shift toward reliance on technology and the internet without adequate awareness infrastructure to mitigate associated risks. The study's results revealed that, despite the students' intensive use of the internet for academic and social purposes, they exhibit a noticeable lack of awareness regarding cybersecurity threats. Phishing attacks, malware, and password-related threats were found to be the most prevalent, largely due to limited knowledge of basic protection mechanisms. The primary aim of this research is to assess students' awareness levels concerning cybersecurity threats and attacks. To achieve this, a quantitative approach was employed, using specially designed questionnaires for data collection. The study involved a sample of 148 students, examining their awareness of cybersecurity threats and their digital behavior.

Keywords— Cyberattacks, Phishing, Electronic Fraud, Password Cracking, Malware, Smishing, Vishing, Ransomware, Trojan, Spyware, Brute Force Attacks, Password Reuse, Insecure Password Storage

I. Introduction

Yemen has experienced a delay in keeping up with technological advancements. For example, 4G technology was launched globally in 2009, whereas it was introduced in Yemen in 2018. Additionally, the satellite internet service "Starlink" recently entered Yemen, sparking widespread debate about its benefits and risks.

This delay, along with the sudden technological advancements in Yemen, has led to weak awareness regarding the proper use of this technology. Consequently, this growth has recently resulted in an increase in the number of users. In 2023, the number of internet users in Yemen reached 9.10 million, accounting for 26.7% of the total population, in addition to 19.63 million active mobile network subscriptions and 3.05 million active social media users [1].

Accordingly, technology has become an essential part of our daily lives. As dependence on the internet increases across various fields, cyberattacks have also escalated. It is crucial for individuals to be aware of these threats and learn how to protect themselves from digital risks. In this context, raising awareness of cyberattacks among students is particularly important, as this group uses technology daily in various academic and research activities.

Therefore, it is essential to enhance awareness of digital threats and provide the necessary training to protect personal information and data from potential risks.

In other words, a lack of awareness of cyberattacks exposes individuals to numerous risks that could negatively impact their personal and professional lives, potentially leading to financial losses, privacy breaches, and even threats and blackmail.

A. Research Problem

Despite the intensive use of technology in their daily lives, students at the University of Science and Technology still suffer from a clear lack of awareness of cyberattacks, exposing them to risks that may negatively affect their academic and personal lives.

Although some awareness programs exist at the University of Science and Technology, they have been limited in scope and have not been generalized to all students, as they were confined to certain classrooms only.

The results of a survey distributed to 1,024 people in Aden showed that the percentage of those who do not know the concept of cybersecurity is 12.01%, while 62.21% have only basic knowledge [2]. This highlights the urgent need to study the weaknesses in students' awareness of cyberattacks and identify the most widespread attacks among them.

University students are the largest group using the internet, and they should be more aware of the risks of cybersecurity and the attacks they face online. Awareness of cybersecurity pitfalls and attacks should begin in the early stages of university education [3]. University students need to secure their academic and personal data to avoid risks and mitigate the potential consequences of cyberattacks, or at least mitigate the effects of these risks [4]. University students' lack of awareness of the threats and risks they may face while using the internet can lead to successful attacks. Students must cultivate a culture of cybersecurity awareness before engaging in any activity.

B. Research Question

RQ1. How does the level of awareness of cyberattacks differ between male and female students at the university? RQ2. What are the most prevalent cyberattacks among students at the University of Science and Technology?

C. Research Objectives

The last user of the Internet is considered a weak link.[5]. Therefore, if students are not sufficiently aware of cybersecurity threats, they cannot be avoided, reported, or prevented. This research aims to evaluate the level of awareness among male and female students at the University of Science and Technology university by identifying the most prevalent cyberattacks among them, from the most to the least common. It also seeks to examine their cybersecurity awareness weaknesses and identify the underlying causes.

D. Research Significance

This research contributes to identifying the areas where students are most vulnerable to cyberattacks, helping to direct awareness efforts toward the most critical aspects. It also aids in developing future awareness programs within the university based on the study's findings regarding the prevalence of attacks among students. Additionally, the research enables university administration to understand the topics students need to learn about to enhance their awareness of cyber threats. Moreover, it provides valuable data on the differences in awareness between male and female students.

E. Research Limitations

a. Temporal Limitations: The research covers the period from January 2, 2025, to April 5, 2025, which is the designated timeframe for data collection and analysis.
b. Geographical Limitations: The study focuses on students of the University of Science and Technology.
c. Methodological Limitations: The research relies on qualitative analysis.
d. Sample Limitations: The sample consists of 148 students.
e. Ethical Limitations: The study adheres to ethical principles of scientific research, ensuring that participants were informed about the nature of the study and that their data remained confidential, with no disclosure of personal information.
f. Subject Matter Limitations: The research does not cover all types of cyberattacks but focuses on several well-known categories that individuals may encounter, including password threats, online fraud, and malware.

F. Definition of Terms

a. **Cyber security:** "is how individuals and organizations reduce the risk of cyber-attack, the main function is to protect devices we use and services we access from theft and damage, and preventing unauthorized access to the vast amount of personal information we store and online." [6]
b. **Cyberattack**: "A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device." [7]
c. **Electronic Fraud**: "involves using online services and software with access to the internet to defraud or take advantage of victims." [8]
d. **Password Cracking**: "Password cracking (also called password hacking) is an attack vector that involves hackers attempting to crack or determine a password for unauthorized authentication." [9]
e. **Malware**: "Malware, short for malicious software, encompasses any intrusive software developed by individuals to steal data, damage, or destroy computers and computer systems." [10]
f. **Phishing**: "Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls, or websites to trick people into sharing sensitive data, downloading malware, or otherwise exposing themselves to cybercrime." [11]
g. **Smishing**: "is a phishing cybersecurity attack carried out over mobile text messaging, also known as SMS phishing." [12]
h. **Vishing**: "is a type of phishing attack that tricks people into sharing sensitive information through telephone calls." [13]
i. **Website Phishing**: "Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details." [14]
j. **Malvertising**: "is a technique that cybercriminals use to inject malware into users' computers when they visit malicious websites or click on an ad online. Malvertising may also direct users to a corrupted website where their data can be stolen or malware can be downloaded onto their computer." [15]
k. **QR code phishing (quishing)**: "is a type of social engineering attack. Cybercriminals try to trick victims into using the camera on their mobile phone to scan a QR code that goes to a malicious website to steal sensitive information, such as login credentials or financial data." [16]
l. **Viruses**: "is a program that spreads by infecting files and making copies of itself. Some viruses are harmless, others may damage data files, and some may destroy files. Viruses used to be spread when people shared floppy disks and other portable media;

now viruses are primarily spread through email messages." [17]

m. **Ransomware**: "is a type malware that holds a victim's sensitive data or device hostage, threatening to keep it locked—or worse—unless the victim pays a ransom to the attacker." [18]
n. **Adware**: "is a type of malware that displays unwanted advertisements on your computer or device." [19]
o. **Trojan**: "is a type of malware typically presented to its victim as legitimate software." [20]
p. **Spyware**: "is a type of malicious software (malware) that is installed on a computing device without the user's knowledge." [21]
q. **Weak Password**: " Those that are easy to guess, either for a human or a computer." [22]
r. **Brute Force Attack**: A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. [23]
s. **Default configurations** are "the settings that come pre-installed on hardware, software, and systems straight out of the box." [24]
t. **Password reuse** is "a person's tendency to use the same password across different online services." [25]
u. **Insecure Passwords Storage**: "Storing passwords in plain text, such as in a document or database, is one of the most insecure methods." [26]

II. Literature Review

Many previous studies have addressed the level of cybersecurity awareness among university students, focusing on the impact of demographic and educational factors.

In study [27], the primary objective was to analyze the level of information security awareness among faculty members, researchers, undergraduate students, and staff in educational environments in the Middle East to understand their awareness of information security risks and their overall impact on institutions. The findings revealed that participants lacked sufficient knowledge and understanding of information security principles and their practical significance in daily life. However, this issue could be addressed through comprehensive awareness and training programs, in addition to adopting all necessary security measures at all institutional levels to ensure that students, faculty members, and staff possess sufficient technological awareness to protect their data.

In study [28], the level of cybersecurity awareness among students at Yobe University in Nigeria was assessed through a questionnaire involving 201 students from the computer science department. The results indicated that students had a generally good awareness level but lacked knowledge about personal data protection, making them more vulnerable to cyberattacks. The study also highlighted the absence of formal awareness programs within the university, which could explain this deficiency in security knowledge.

Similarly, a study conducted in Saudi Arabia [29] found that the level of cybersecurity awareness among university students was moderate, with no significant gender differences. However, female students showed greater interest in the topic compared to their male counterparts. The study also found that students specializing in computer science and information technology had higher awareness levels than those in other disciplines. Additionally, the results indicated that students in urban areas were more knowledgeable about cyber risks than those in rural areas, reflecting the role of geographical environment in shaping cybersecurity awareness.

In a recent study [30], cybersecurity awareness among university students in northeastern Nigeria was analyzed,

focusing on topics such as cyberbullying, self-protection, and online banking transactions. The study found that students had good knowledge of secure online banking transactions, while their awareness of cyberbullying risks and internet addiction was moderate. Furthermore, the study showed that 77.1% of the participants were male, which may indicate differences in awareness levels and engagement between genders.

In study [31], students' awareness of cybersecurity threats was assessed, along with their problem-solving skills and ability to interact with complex systems using a questionnaire-based approach. The survey included 352 students and covered subtopics such as general knowledge of malware, password usage, and social media. The study aimed to identify key gaps in current cybersecurity knowledge to improve awareness, training, and education programs. The results revealed that students' cybersecurity knowledge was somewhat advanced, but their ability to apply this knowledge in real-life situations was weak.

This review highlights the development of research on students' cybersecurity awareness in recent years. Study [27], conducted in 2016, emphasized the lack of knowledge about information security principles among students, faculty, and staff in educational environments in the Middle East, proposing training programs to address this gap. Study [28], conducted in 2020, focused on the absence of awareness programs at Yobe University in Nigeria and indicated that students lacked knowledge of personal data protection. In contrast, study [29], in 2021, revealed variations in cybersecurity awareness levels across disciplines and geographical regions in Saudi Arabia, noting a greater interest in the topic among female students. Study [30], in 2022, stressed the need for more comprehensive awareness programs, particularly concerning the risks of cyberbullying and internet addiction. Finally, study [31], conducted in 2024, confirmed that cybersecurity awareness among students in Jordan was somewhat advanced but weak in practical application, highlighting the need for improvements in training and education programs in this field.

III. METHODOLOGY

In this study, we adopted a quantitative approach to design the questionnaire for collecting and analyzing data related to the awareness of students at the University of Science and Technology – regarding cyberattacks. The objective of employing the quantitative method is to measure the level of awareness of cyber threats in an objective and measurable manner, allowing for statistically analyzable results and deriving differences among the targeted groups.

A. Data Collection Methods

The primary data source for this study is the questionnaire, which was designed to cover various types of cyberattacks targeting students at the University of Science and Technology. A total of 148 responses were collected using two types of questionnaires:

a. An electronic questionnaire via Google Forms, which was distributed to students through email or social media platforms.
b. A paper-based questionnaire distributed on campus to ensure that all students, including those who may not have continuous internet access, could participate.

B. Questionnaire Design

The questionnaire was designed in a way that does not require participants to provide any sensitive information, such as names, ensuring their privacy and enhancing the credibility of their responses. Participants were also clearly informed about the research's objectives and significance, giving the questionnaire a formal character that reinforces the accuracy of the collected data.

The questionnaire consists of 18 questions divided into four main sections:

a. Demographic data (3 questions)
b. Electronic fraud (5 questions)
c. Malware (5 questions)
d. Passwords (5 questions)

The threats were explained through a hypothetical scenario in a simple and clear manner, facilitating participants' understanding of the questions. The estimated time required to complete the questionnaire ranges from 5 to 10 minutes.

After collecting the responses, the data was analyzed using Excel software, where descriptive statistical analysis was applied to determine students' exposure to cyberattacks and their awareness of them.

C. Data analysis:

After data collection, statistical tools available in Excel will be used to conduct quantitative analysis. This includes:

a. Frequency analysis to identify demographic distribution by gender and age, as well as to calculate operating system usage and the occurrence of each threat.
b. Relative comparison to determine differences between genders.
c. Arithmetic Mean to measure the intensity of exposure to attacks.

Through this approach, we will obtain accurate and comparable results. These findings will help identify areas that require improvement in cybersecurity awareness programs at the university.

IV. RESULTS AND DISCUSSION

The data extracted from the questionnaire was analyzed using Excel to assess the awareness of University of Science and Technology students regarding cyberattacks. The questionnaire was designed to cover four main sections: demographic data, online fraud, malware, and password threats. A total of 148 students participated in the survey, providing a suitable sample to derive statistically significant conclusions about students' awareness of cybersecurity threats.

A. Demographic Data

Table 1: Participants by Gender

Gender	Frequency	Percentage
Male	88	59.5%
Female	60	40.5%

Table 2: participants by age

Gender	<18	18-25	26-35	36-45	>45
Male	2	80	0	0	0
Female	5	58	0	3	0

Table 3: Participants by Operating System

Gender	Total	Android	iOS	Windows	MacOS	Linux
Male	88	54	21	31	1	7
Female	60	35	25	21	1	1

The results showed that 59.5% of the participants were male, while females constituted 40.5%. The demographic data also indicated that the vast majority of participants were aged 18 to 25 years, representing 80.41% of the total, which reflects that most of the sample consists of the target age group for university education.

Regarding the operating systems used, Android was the most commonly used among participants, with 89 students (54 males and 35 females) using it, followed by Windows, used by 52 students. On the other hand, the usage rates of MacOS and Linux were very low among students, indicating their limited use in academic environments.

B. Phishing Attacks

Table 4: Phishing Attacks

Attack Type	**Male**	**Female**
Total	88	**60**
Attack victims	Yes	**Yes**
Smishing	47	**44**
Vishing	39	**18**
Web Phishing	33	**26**
Malvertising	65	**35**
QR Code	**31**	**26**

The analysis results indicate that malvertising was the most common fraudulent attack among participants, affecting 100 individuals, making it the most widespread threat. This was followed by smishing (phishing via text messages) with 91 victims and web phishing, which affected 59 individuals. Meanwhile, vishing (voice phishing) and QR code phishing each impacted 57 individuals.

When comparing the targeting of males and females, the data showed that females were more vulnerable to smishing (73.3%), web phishing (43.3%), and QR code phishing

(43.3%) compared to males. On the other hand, males were more exposed to vishing (44.3%) and malvertising (73.9%). Additionally, the findings revealed that the average number of phishing attacks per individual was 2.46, with a slight difference between males (2.44) and females (2.48). This suggests that both genders are nearly equally targeted in cyber fraud operations, although certain attacks appear to be more concentrated on specific demographics.

C. Malicious Software

Table 5: Table Type Styles

Attack Type	Male	Female
Total	88	60
Attack victims	Yes	Yes
Virus	64	31
Ransomware	5	5
Adware	59	40
Trojans	50	27
Spyware	61	36

The analysis results showed that the most common type of malicious software attacks among participants was adware, with 99 reported cases, followed by spyware with 97 cases, and then viruses with 95 cases. Trojans were reported in 77 cases, while ransomware was the least common attack, with only 10 cases recorded.

When comparing the impact of these attacks between males and females, the data indicated that males were more affected by most threats, with higher exposure to viruses (72.7%), Trojans (56.8%), and spyware (69.3%) compared to females. The prevalence of adware was quite similar between genders, with 67.0% of males and 66.7% of females being affected. As for ransomware, females had a slightly higher incidence (8.3% compared to 5.7% in males).

In terms of the average number of attacks per individual, males experienced an average of 2.7 attacks, while females were affected by an average of 2.3 attacks, making the overall average for all participants 2.6 attacks per person. This indicates that malicious software attacks are widespread, with varying patterns of targeting between males and females, where males appear more susceptible to more complex attacks such as viruses and Trojans, while the levels of exposure to adware attacks were more evenly distributed between genders.

D. Password Threats

Table 6: Password Threats

Threat Type	Male	Female
Total	88	60
Those who were threatened	Yes	Yes
Weak Passwords	53	40
Brute Force Attacks	40	24
Default Passwords	48	20
Password Reuse	67	41
Saving Passwords Unsafely	58	32

The analysis results revealed that password reuse was the most common threat among participants, with 108 recorded cases, highlighting a widespread behavior that increases the risk of security breaches. This was followed by weak passwords with 93 cases, then saving passwords unsafely with 90 cases. Default passwords were reported in 68 cases, while brute force attacks were the least common, with 64 cases recorded.

By analyzing gender differences, the data showed that females were more vulnerable to weak passwords (66.7%) compared to males (60.2%). However, males were more exposed to most other threats, especially default passwords (54.5% for males vs. 33.3% for females), marking the largest gender gap (+21.2%) among all recorded differences. Additionally, males reported higher rates of brute force attacks (45.5%), password reuse (76.1%), and saving passwords unsafely (65.9%).

Regarding the average number of threats per individual, males experienced an average of 3.1 threats, while females faced an average of 2.7 threats, leading to an overall average of 2.9 threats per participant. These findings indicate that all participants face repeated security risks related to password management, with variations in threat patterns between genders. Females struggle more with weak passwords, whereas males encounter greater risks from password reuse and unsafe storage practices.

E. Overall Summary

a. Ranking of Cyber Threats from Most to Least Common

Table 7: Table Type Styles

Threat	**Cases**	**Category**	**Male**	**Female**	**Gender Difference**
1	Password Reuse	108	Threats	76.1%	68.3%
2	Malvertising	100	Phishing	73.9%	58.3%
3	Adware	99	Malware	67.0%	66.7%
4	Spyware	97	Malware	69.3%	60.0%
5	Viruses	95	Malware	72.7%	51.7%
6	Weak Passwords	93	Threats	60.2%	66.7%
7	Smishing	91	Phishing	53.4%	73.3%
8	Unsafe Pass Storage	90	Threats	65.9%	53.3%
9	Trojans	77	Malware	56.8%	45.0%

10	Default Passwords	68	Threats	54.5%	33.3%
11	Brute Force Attacks	64	Threats	45.5%	40.0%
12	Web Phishing	59	Phishing	37.5%	43.3%
13	Vishing	57	Phishing	44.3%	30.0%
14	QR Code Phishing	57	Phishing	35.2%	43.3%
15	Ransomware	10	Malware	5.7%	8.3%

A. Predominant Threat Patterns

Password management issues top the list of cyber threats, with "password reuse" being the most widespread (108 cases), followed by "unsafe password storage" (90 cases) and "weak passwords" (93 cases). These findings reflect a systemic weakness in digital practices, making individuals more vulnerable to breaches. In the malware category, "malvertising" (100 cases) and "viruses" (95 cases) emerge as the most prominent threats, indicating a lack of technical protection tools and secure browsing awareness. Meanwhile, phishing attacks vary between SMS phishing (91 cases) and web phishing (59 cases), with a clear gender-based disparity in targeting.

B. Gender Differences in Exposure to Threats

Males are more exposed to "technical threats" such as viruses (+21.0%), spyware (+9.3%), and default passwords (+21.2%). This can be attributed to behaviors like downloading software from untrusted sources or neglecting system updates. Females are more vulnerable to "direct communication threats" such as SMS phishing (-19.9%) and QR code phishing (-8.1%), possibly due to higher trust in text messages or social media interactions. Exposure to adware is nearly identical between genders (67.0% for males vs. 66.7% for females), indicating that this threat is widespread and not gender-specific.

C. Cyberattack frequency per person

a. Phishing
   - Average Exposure: 2.44 attacks per individual (males) | 2.48 attacks per individual (females)
   - Gender Gap: -0.04 in favor of females (minimal difference)
   - Key Threats: Malvertising (100 cases), SMS Phishing, Smishing (91 cases)

b. Malware
   - Average Exposure: 2.7 attacks per individual (males) | 2.3 attacks per individual (females)
   - Key Threats: Adware (99 cases), Viruses (95 cases)

c. Password Security Threats
   - Average Exposure: 3.1 attacks per individual (males) | 2.7 attacks per individual (females)
   - Key Threats: Password Reuse (108 cases), Unsafe Password Storage (90 cases)

d. Total Exposure to Cyber Threats
   - Overall Average Per Individual: 7.9 attacks. Males:
   - 8.2 attacks per individual, Females: 7.5 attacks per individual
   - Total Recorded Attacks: 1,165 attacks

D. Less Prevalent Threats

Ransomware recorded the lowest occurrence, with only 10 cases. This may indicate its relative rarity or the increased difficulty of execution compared to other threats. However, its potential severity, particularly in compromising sensitive data, cannot be overlooked.

E. Recommendations:

Based on the results of the study, which showed a weakness in cybersecurity awareness among students at the University of Science and Technology due to the lack of awareness activities and the students' lack of knowledge on how to protect their personal data, the study recommends the following:

a. The university administration is recommended to organize no less than two awareness lectures annually, at the beginning of each academic semester, targeting students of all specializations, with the aim of raising the level of awareness regarding personal information security and methods of protection from cyber threats.
b. It is suggested to distribute guidance booklets to students at the beginning of each academic year containing simplified tips and instructions for data protection and dealing with electronic threats.
c. It is recommended to periodically publish awareness content on the most common cyber threats among students on the university's official social media accounts, including articles, infographics, and short videos.
d. The student should verify the sources of email messages before opening or interacting with them; to verify the source of emails, it is advised to use the site mxtoolbox.com.
e. It is preferred that the student verify unknown phone numbers using websites such as WhoCallsMe.com or Truecaller.com, in order to check numbers that have been previously reported.
f. The student should avoid interacting with unknown links without scanning them; it is recommended to use VirusTotal.com.
g. The student should use security software such as Kaspersky and ensure it is updated automatically in order to provide continuous protection from malicious software and harmful advertisements.
h. The student should download applications only from official websites or stores of the developing companies, for example, Microsoft Store, Google Play, App Store and avoid using unknown download

sites or pirated versions in order to reduce the risk of installing malicious or spyware programs.

i. The student should follow safe steps before installing any application, including reviewing user reviews to avoid installing adware programs, reading the terms of use carefully before granting any permissions, and restricting the permissions granted to applications to match their actual functions.
j. The student is advised not to reuse the same password for more than one account and to rely on password management tools such as Bitwarden and LastPass.
k. It is important that students commit to using strong and unique passwords.
l. It is preferred that the student change default passwords.
m. The student should not interact with suspicious messages or calls from unknown sources and report them when necessary.

V. CONCLUSION:

This study examined cyberattack awareness among UST students, highlighting the impact of Yemen's delayed technological advancements on cybersecurity knowledge. Findings indicate a lack of awareness regarding cyber threats and safe online practices, emphasizing the need for targeted educational initiatives. Our research contributes to cybersecurity awareness but is limited in scope, warranting further studies on effective training programs. To enhance students' digital safety, universities should promote awareness campaigns and prioritize workshops, seminars, and training sessions on cybersecurity. Strengthening cyber awareness is crucial in equipping students to navigate the digital world securely.

REFERENCES

[1] S. E. Erol and S. Sagiroglu, "Awareness Qualification Level Measurement Model," in *Int. Congr. Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, Dec. 2018.

[2] M. Jaber, M. Dhaini, A. Fakherddine, and R. A. Haraty, "A Novel Privacy-Preserving Healthcare Information Sharing Platform Using Blockchain," in *Security and Privacy Issues in IoT Devices and Sensor Networks. Advances in Ubiquitous Sensing Applications for Healthcare*, Elsevier, 2021, pp. 245–261.

[3] National Cyber Security Centre (NCSC), "What is cyber security?" [Online]. Available: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[4] IBM, "What is a cyberattack?" [Online]. Available: https://www.ibm.com/think/topics/cyber-attack

[5] Fortinet, "What is Internet fraud? Types of Internet fraud," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/internet-fraud

[6] BeyondTrust, "Password cracking 101: Attacks & defenses explained," [Online]. Available: https://www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained

[7] Cisco, "What is malware? Definition and examples," [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html

[8] IBM, "What is phishing?" [Online]. Available: https://www.ibm.com/think/topics/phishing

[9] Kaspersky, "What is smishing, and how to defend against it," [Online]. Available: https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[10] Cloudflare, "What is vishing?" [Online]. Available: https://www.cloudflare.com/it-it/learning/email-security/what-is-vishing/

[11] TechTarget, "What is phishing? How does it work? Prevention, examples," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/phishing

[12] Fortinet, "What is malvertising and how to prevent it?" [Online]. Available: https://www.fortinet.com/resources/cyberglossary/malvertising

[13] Barracuda, "Threat spotlight: The evolving use of QR codes in phishing attacks," [Online]. Available: https://blog.barracuda.com/2024/10/22/threat-spotlight-evolving-qr-codes-phishing-attacks

[14] Cybersecurity & Infrastructure Security Agency (CISA), "Virus basics," [Online]. Available: https://www.cisa.gov/news-events/news/virus-basics

[15] IBM, "What is ransomware?" [Online]. Available: https://www.ibm.com/think/topics/ransomware

[16] ESET, "What is adware and how can you avoid it?" [Online]. Available: https://www.eset.com/uk/types-of-cyber-threats/adware/

[17] VIPRE, "What is a Trojan virus? Examples & definitions," [Online]. Available: https://vipre.com/glossary-terms/what-is-a-trojan-virus/

[18] TechTarget, "What is spyware?" [Online]. Available: https://www.techtarget.com/searchsecurity/definition/spyware

[19] ScienceDirect, "Weak password – An overview," [Online]. Available: https://www.sciencedirect.com/topics/computer-science/weak-password

[20] Wikipedia, "Brute force attacks," [Online]. Available: https://en.wikipedia.org/wiki/Brute-force_attack

[21] Critical Start, "Default configurations: A common gateway for threat actors," [Online]. Available: https://www.criticalstart.com/default-configurations-a-common-gateway-for-threat-actors/

[22] HYPR, "What is a password reuse attack?" [Online]. Available: https://www.hypr.com/security-encyclopedia/password-reuse
[23] CQR, "Insecure password storage," [Online]. Available: https://cqr.company/web-vulnerabilities/insecure-passwords-storage/
[24] S. Al-Janabi and I. Alshourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, 1650007, 2016, doi: 10.1142/S0219649216500076.
[25] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa, "A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach," *Int. J. Emerg. Technol.*, vol. 11, no. 5, pp. 41–49, 2020.
[26] W. Aljohni, N. Elfadil, M. Jarajreh, and M. Gasmelsied, "Cybersecurity awareness level: The case of Saudi Arabia university students," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 3, pp. 276–281, 2021.
[27] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 12, no. 1, pp. 572–584, 2022.
[28] B. Muasher, A. Ghandour, and H. Abusaimeh, "Enhancing Digital Transformation in Higher Education: A Study on Cybersecurity Awareness Among University Students in Jordan with a Case Study at Middle East University," in *Studies in Big Data*, pp. 137–149, 2024, doi: 10.1007/978-3-031-73632-2_12.