Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

# CYBERSECURITY AWARENESS AMONG UNIVERSITY STUDENTS: A CASE STUDY OF QAIWAN INTERNATIONAL UNIVERSITY

**Hakar Mohammed Rasul[*1], Zhyar Yassin Abdalla[2], Nur Haryani Zakaria[3], Sasan Sarbast Abdalkhaliq[4]**

[*1,2,4]*Faculty of Engineering and Computer Sciences, Qaiwan International University, Sulaymaniyah, Iraq*
[1,2]*Computer Science Department, Kurdistan Technical Institute Sulaimani, Iraq*
[3]*Schoolof Computing, Universiti Utara Malaysia, 06010 Sintok, Kedah, Malaysia*

[*1]hakar.raswl@uniq.edu.iq, [2]zhyra.yassin@uniq.edu.iq, [3]haryani@uum.edu.my , [4]sasan.sarbast@uniq.edu.iq

DOI: https://doi.org/10.5281/zenodo.19333161

**Keywords**
*Cybersecurity awareness, university students, phishing attacks, information security, higher education, cybersecurity training.*

**Article History**
*Received: 31 January 2026*
*Accepted: 14 March 2026*
*Published: 30 March 2026*


**Corresponding Author: ***
**Hakar Mohammed Rasul**

## Abstract

*Higher Education institutions have seen a large shift to digital systems in recent years and as such, students have become increasingly susceptible to various types of cyber threats including but not limited to: phishing, identity theft, and malware infection. Although numerous Universities utilize digital systems to provide services and educational materials to students, it is just as important today as it has ever been to make sure students understand the importance of Cybersecurity Awareness. This research will assess the level of Cybersecurity Awareness among students at Qaiwan International University through a quantitative methodology using an online survey to gather responses from 356 students across five Faculties: Dentistry, Pharmacy, Engineering & Computer Science, Health Sciences, and Management & Social Sciences. The Survey instrument contained questions to assess students' knowledge, practices, and attitudes toward Cybersecurity. Descriptive Statistics, Correlation Analysis, and Analysis of Variance (ANOVA) were utilized to analyze the collected data. Results showed that students have a low level of Cybersecurity Knowledge (M = 2.06), and demonstrate a lack of Cybersecurity Practices (M = 1.86). Students reported moderate attitudes toward Cybersecurity. Further, 60.1% of respondents admitted to being unaware of Phishing Attacks which demonstrates a significant deficiency in the understanding of commonly encountered cyber threats by students. Results indicated that students that have received training in Cybersecurity demonstrated a greater level of awareness when compared to those that have not. Additionally, there were no major differences in levels of awareness across the various Faculties. The study highlights the need to integrate Cybersecurity Education and Awareness Programs into University Curriculum in order to enable students to better recognize and defend against cyber threats.*

## INTRODUCTION

A large number of universities now use digital technologies for delivery of education, communication with students and for administrative purposes. As a result, modern higher education institutions are now largely dependent on online systems and applications such as Learning Management Systems, Student Information Systems, Digital Libraries and Cloud-Based Collaboration Tools. Although these technologies make it easier for students to be able to access courses and other resources, they also

create new risks for the students and the institution such as phishing attacks, malware infection, identity theft and unauthorized access to sensitive data (Hadlington, 2017; Parsons et al., 2017). The increased reliance by students on digital systems for academic and personal reasons makes awareness of cyber threats a major concern for both the safety of individuals and the protection of the institution.

Cybersecurity Awareness is defined as an individual's knowledge, attitudes and practices regarding the protection of digital information and systems against cyber threats (Kruger & Kearney, 2006). Studies have previously demonstrated that technology-based solutions alone will not ensure adequate protection for information systems when the users lack sufficient knowledge and/or ability to identify and react to cyber threats. Human factors have been identified as one of the greatest vulnerabilities in cybersecurity. Many cyber incidents occur due to the actions of users such as using weak passwords, clicking on malicious links or sharing confidential information over the internet (Parsons et al., 2017). Therefore, enhancing the awareness of cybersecurity issues among students represents a key area for universities to focus on in terms of developing their own cybersecurity strategies.

Students represent a highly relevant group in the field of cybersecurity. Students often access various online resources via multiple devices and networks, e.g. laptop computers, mobile phones and public WIFI connections. As a result, students experience a much greater degree of exposure to cyber threats than the general public. Additionally, many students do not receive formal training in cybersecurity, which makes them even more susceptible to attacks such as phishing and social engineering (Yan et al., 2018; Alharbi & Tassaddiq, 2021; Shahbazi et al., 2025). A number of studies have reported that students tend to have positive attitudes toward cybersecurity, but their actual security practices remain inadequate (Bada & Nurse, 2019).

Among the numerous types of cyber threats, phishing attacks are considered one of the most prevalent threats to university students. Phishing attacks usually take the form of fake emails or web sites designed to deceive users into providing sensitive information, e.g. passwords or financial data. Research has indicated that a substantial proportion of students are unable to properly identify phishing attempts, indicating a need for improvement in awareness and training programs (Sheng et al., 2010). Therefore, universities have a significant responsibility in informing students about cyber threats and teaching them how to behave responsibly online.

Although there is increasing recognition of the importance of raising students' awareness of cybersecurity issues, relatively little research has focused specifically on the level of awareness among university students in the Kurdistan Region of Iraq. As higher education institutions in the region are progressively implementing digital technologies, it is essential that the knowledge and behaviors of students regarding cybersecurity are understood in order to develop successful awareness programs. Identifying the current level of students' knowledge and behaviors will enable universities to assess the existing gaps and design targeted education programs to improve students' preparedness for cyber threats.

The purpose of this study is to investigate students' level of cybersecurity awareness at Qaiwan International University. Specifically, this study examines students' cybersecurity knowledge, security practices, attitudes toward cybersecurity and the differences in awareness between different academic faculties and whether cybersecurity training impacts students' awareness levels. Ultimately, this study aims to provide insights to support universities in developing effective cybersecurity awareness programs and strengthening the overall security culture in higher education institutions.

This study aims to find out how aware university students are about Cybersecurity. The study has four main objectives:

1. To assess how much Cybersecurity knowledge the average university student has.
2. To evaluate how well students practice Cybersecurity on a day-to-day basis with their Digital Activities.
3. To examine whether there are any significant differences in the amount of

Cybersecurity knowledge that students have depending on which Academic Faculty they are studying at.

4. To analyze if taking a Cybersecurity course will affect the way students think about Cybersecurity and practice it.

In order to meet the goals listed above, the study asks the following Research Questions:

1. What is the overall level of Cybersecurity awareness of university students?
2. How well do students understand phishing and other forms of cyber threats that happen over the Internet?
3. Can Cybersecurity training increase the overall level of Cybersecurity awareness in students?
4. Are there any statistically significant differences in the Cybersecurity awareness levels of students from different faculties?

## LITERATURE REVIEW

### Cybersecurity Awareness:

Modern society's dependence on digital technology has greatly increased the vulnerability of cyber threats (Saeed et al., 2023; World Economic Forum, 2025). University campuses rely heavily upon digital systems for teaching, research, communications, and administrative functions (Barrett, 2024; Fernández et al., 2023). These technological advancements provide increased efficiency and accessibility; however, they also increase the risk of cybersecurity concerns. Because of this, cybersecurity awareness is now an important method of protecting institutional systems and user data (Fouad, 2021; Fernández et al., 2023).

Cybersecurity awareness generally describes an individual's knowledge of cyber threats and how they use safe practices when using digital technologies (Kruger & Kearney, 2006). Cybersecurity awareness includes knowledge of the potential risks, individual's views on information security, and individual's behaviors that help to prevent cybercrime. Scholarly research emphasizes that technological defenses will be ineffective at reducing cyber risks without sufficient cybersecurity awareness and the willingness of users to utilize safe behaviors (Parsons et al., 2017). Often times, human error is identified as one of the most common reasons for cybersecurity breaches.

Studies show that increasing an individual's level of cybersecurity awareness can substantially decrease an individual's exposure to security risks (Prümmer et al., 2024; Chahid et al., 2026). Cybersecurity awareness programs assist individuals in recognizing suspicious activities, understanding security policies, and adopting safer digital behaviors (Prümmer et al., 2024; Alshammari et al., 2025). Due to the fact that many organizations and educational institutions are identifying the need for increased cybersecurity awareness, many have initiated cybersecurity awareness programs as part of their larger security strategy (Bada & Nurse, 2019).

### Cybersecurity Awareness Among University Students

University students represent a unique demographic when it comes to cybersecurity awareness. Many university students access institutional systems, personal email accounts, and online services using numerous devices and networks (Yan et al., 2018; Pósa et al., 2022; Alrobaian et al., 2023). Accessing these types of systems and services exposes students to a variety of cyber threats, including but not limited to phishing attacks, malware infections, and data breaches (Dolliver et al., 2021; EDUCAUSE, 2021).

Several studies have examined cybersecurity awareness among university students and have reported low levels of awareness. One study (Hadlington, 2017) found that many students engaged in high-risk online behaviors such as reusing passwords, sharing personal identifiable information online, and failing to update software. Although many university students understand the importance of cybersecurity, many of their actions reflect a lack of adherence to accepted security best practices.

Another study (Hadlington, 2017) found that students enrolled in technical disciplines did not report higher levels of cybersecurity awareness than students enrolled in non-technical disciplines. This indicates that cybersecurity

knowledge does not equate to cybersecurity behavior absent of additional education and ongoing awareness programs. Thus, universities should make certain that cybersecurity education is provided to students regardless of their field of study.

**Cybersecurity Knowledge**

Cybersecurity knowledge describes an individual's understanding of digital security concepts, cyber threats, and protective methods (Ahamed et al., 2026; IBM, 2025). This knowledge includes familiarity with issues like phishing, password security, malware, and data protection practices. An individual's knowledge of these issues directly impacts their ability to identify potential threats and react accordingly.

Research continually demonstrates that individuals who possess greater levels of cybersecurity knowledge are more likely to perform safe online behaviors. Kruger and Kearney (2006) argue that knowledge is a major component of cybersecurity awareness frameworks which contribute to the development of safe online behaviors. The more an individual understands the risks associated with digital systems, the more likely he/she is to take preventative measures, such as creating strong passwords, verifying suspicious emails, and avoiding sites known to pose a threat (Arachchilage & Love, 2014; Kennison & Chan-Tin, 2020).

Despite the continual emphasis on cybersecurity knowledge within academia, research shows that many university students only have a rudimentary knowledge of cybersecurity. Specifically, university students commonly lack the knowledge to recognize complex cyber threats such as phishing, social engineering, etc. Lack of knowledge increases the probability that students will unknowingly place themselves or institutional systems at risk of cyber threats.

**Cybersecurity Practices**

A large number of students, although informed of the risks, do not practice good cybersecurity. Convenience, a lack of motivation, or an underestimation of the risks are some reasons why people do not practice good cybersecurity even though they know the risks (Alharbi et al., 2021; Han et al., 2025; Setiawan et al., 2023). An example of this would be when someone uses the same password on multiple sites, knowing that there is a risk, yet doing so anyway.

Poor cybersecurity practices from students will increase the risk for institutional networks to be vulnerable. By accessing the university's network via a poorly secured device, or by having a weak password to access the university's system, a student could potentially release sensitive information without realizing it. Improving the cybersecurity practices of students is an important step in increasing the cybersecurity resiliency of the institution.

**Cybersecurity Attitudes**

Cybersecurity attitudes are individuals' perspectives, views and motivations concerning cybersecurity matters. Views towards cybersecurity affect what types of perceived threats individuals believe exist, as well as how likely individuals are to take action to protect themselves from those threats (Alanazi et al., 2022; Han et al., 2025).

Studies have proven that if an individual has a positive view of cybersecurity, they will be more likely to engage in safe digital practices. Users that perceive cyber threats to be serious, and understand the importance of cybersecurity, are more likely to follow security guidelines and implement protective measures to safeguard their digital environment (Bada & Nurse, 2019).

Students generally tend to overestimate their ability to avoid becoming victims of cyberattacks. This is known as an "optimistic bias." The optimistic bias can decrease the amount of motivation to follow security recommendations. Therefore, awareness campaigns need to educate users not only about cybersecurity risks, but also to alter the user's perception of the severity of the risks.

Phishing attacks are the most prevalent form of cyberattack that target both individuals and institutions.

**Phishing Awareness**

A phishing attack is commonly defined as a type of scam that utilizes false e-mails, instant messaging, etc., to obtain sensitive information from users such as usernames and passwords, credit card numbers, etc.

Because university students frequently utilize e-mail services and other online services, university students are one of the most common groups to be targeted in phishing attacks. There have been numerous studies conducted that demonstrate that many students have difficulty distinguishing phishing attempts from legitimate communications from the university (Sheng et al., 2010). Because of this, the necessity for the development of targeted training programs to enhance phishing awareness is evident.

By providing students with knowledge on the indicators of phishing (e.g. suspicious link, suspicious sender address, urgency of obtaining information), the probability of falling victim to a successful phishing attack will be reduced.

**Effect of Cybersecurity Training**

Cybersecurity training is essential to educating individuals on cybersecurity best practices, and to enhancing their awareness of cyber threats. Cybersecurity training usually provides individuals with hands-on instruction on how to identify cyber threats, how to protect their digital account(s) and how to respond to security incidents.

Numerous studies have demonstrated that individuals that participate in cybersecurity training exhibit increased awareness of cyber threats and are more likely to adhere to recommended security best practices (Parsons et al., 2017; Arachchilage & Love, 2014). Furthermore, training may also increase an individual's confidence in being able to identify threats and respond appropriately to suspicious activity.

Despite the numerous benefits of receiving cybersecurity training, numerous university students have not participated in formal cybersecurity training. Thus, incorporating cybersecurity education into the curriculum at universities will assist students in developing necessary digital security skills. Training programs can be provided through workshops, online modules, and awareness campaigns that advocate safe online practices.

## CONCEPTUAL MODEL

Cybersecurity awareness has been widely regarded as a multi-dimensional construct that is shaped by a variety of behavioral and cognitive factors. A number of studies have demonstrated that individual's cybersecurity awareness is shaped by their level of knowledge regarding cyber threats, their attitude towards information security, and their adherence to security practices in their daily digital activities (Kruger & Kearney, 2006; Parsons et al., 2017). In the context of post-secondary institutions, these factors are critical due to the fact that university students spend considerable time engaging with online systems, digital learning platforms, and institutional information systems.

The proposed conceptual framework for this study is based on a tripartite model consisting of three primary dimensions of cybersecurity awareness: cybersecurity knowledge, cybersecurity attitudes, and cybersecurity practices. These dimensions were selected as key predictors of overall cybersecurity awareness among university students.

Cybersecurity knowledge represents students' ability to comprehend digital security concepts, identify common cyber threats and implement appropriate protective measures. An individual's knowledge of cybersecurity enables them to recognize potential risks and respond accordingly to suspicious digital activity. For example, if a student understands the threat posed by phishing attacks, malware, and password vulnerabilities, it is likely they will be able to identify malicious activity and prevent themselves from participating in risky digital behaviors.

Cybersecurity practices represent the specific security behaviors that individuals exhibit while utilizing digital technologies. Examples of these practices include: establishing strong passwords, refraining from opening suspicious emails or clicking on unknown links, maintaining up-to-date versions of software, and safeguarding sensitive personal data. While knowledge serves as the theoretical foundation for understanding the

risk associated with various types of cyber threats, practice demonstrates how individuals utilize that knowledge in real world situations. Studies have illustrated that poor security practices (e.g., utilizing identical passwords across multiple accounts or disregarding system security warnings) significantly enhance an individual's susceptibility to cyber threats.

Cybersecurity attitudes represent an individual's perception, belief, and motivation related to information security. If a student possesses positive attitudes towards cybersecurity, it is likely they will adhere to established security best practices and consider digital threats serious. When students view cybersecurity as an important concern and believe that taking proactive steps to protect against digital threats is vital, they are more likely to engage in safe digital behaviors.

Therefore, the current study proposes that together cybersecurity knowledge, cybersecurity practices, and cybersecurity attitudes collectively contribute to the overall cybersecurity awareness of university students. By comprehending the relationship between these variables, universities can develop effective awareness campaigns and educational initiatives designed to enhance students' preparation for engaging in digital environments securely.

Figure 1 is a representation of the conceptual model used in the current study. This model depicts cybersecurity knowledge, cybersecurity practices, and cybersecurity attitudes as separate independent variables that affect the single dependent variable, overall cybersecurity awareness.

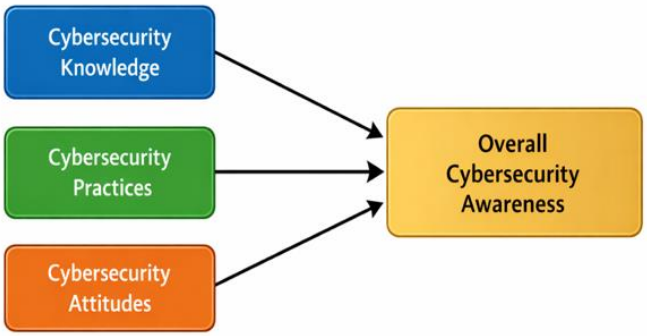


**Figure 1 Conceptual Model of Cybersecurity Awareness**

### Research Hypotheses

Based on the conceptual model, the following hypotheses are proposed:

H1: Cybersecurity knowledge positively influences cybersecurity awareness among university students.

H2: Cybersecurity practices positively influence cybersecurity awareness among university students.

H3: Cybersecurity attitudes positively influence cybersecurity awareness among university students.

## METHODOLOGY

### Quantitative Methods

The current study uses a quantitative methodology to evaluate cybersecurity awareness among students attending universities. The study has utilized the survey method to gather information about the student's cyber security knowledge; their cyber security practices; as well as their cyber security attitudes. Parsons et al. (2017) stated that due to the fact that a quantitative methodology allows researchers to assess the perception and behavior of a large sample, it is frequently used in the evaluation of Cyber Security Awareness in relation to Cyber Security Studies.

The research focuses on assessing students' cybersecurity awareness and examining how knowledge, practices, and attitudes contribute to overall awareness levels.

**Population and Sample**

The population of the study comprises all the full-time undergraduate students registered at Qaiwan International University. Students from five colleges were included in the study:

- Faculty of Dentistry
- Faculty of Pharmacy
- Faculty of Engineering & Computer Science
- Faculty of Health Sciences
- Faculty of Management & Social Sciences

In total, 356 students completed the study. The sample size was determined by an online questionnaire delivered through the university's communication systems. The selected sample size is sufficient for statistical analysis and is common in survey-based studies within the field of higher education.

**Data Collection Instrument**

A structured questionnaire was developed via Google Forms to collect data from participants in this study. The questionnaire was created by examining previous research related to cybersecurity awareness and adapting it for the University setting.

There were four major parts to the questionnaire:

Section 1: Demographics

This part collected general information regarding each respondent, which included:

a. Faculty/Staff or Student
b. Prior cybersecurity training received

Section 2: Cybersecurity Knowledge

This section examined how well the participants understood different aspects of cybersecurity knowledge, such as:

a. Phishing attacks
b. Password Security
c. Malware/Cyber Threats

Section 3: Cybersecurity Practices

This part evaluated the level of secure behavior practiced by participants regarding their overall security practices, which included:

a. Password Management
b. Practices when receiving suspicious emails
c. Overall online safety practices

Section 4: Cybersecurity Attitude

This part of the questionnaire evaluated participants' perception/beliefs of the significance of cybersecurity.

**Measurement Scale**

The survey items were measured using a five-point Likert scale, which is widely used in behavioral and social science research.

The scale ranged from:

| Scale Value | Response Option |
|---|---|
| 1 | Strongly Disagree |
| 2 | Disagree |
| 3 | Neutral |
| 4 | Agree |
| 5 | Strongly Agree |

Higher scores indicate stronger cybersecurity awareness and more secure digital behaviors.

**Data Analysis**

The collected data were analyzed using Python statistical analysis tools and standard statistical techniques. The analysis involved several stages.

- **Descriptive Statistics**

Descriptive statistics were used to summarize the characteristics of the respondents and measure the central tendency of cybersecurity awareness constructs. These statistics included:

- mean
- standard deviation
- minimum and maximum values

Descriptive analysis helped identify the general level of cybersecurity knowledge, practices, and attitudes among students.

- **Faculty Comparison Analysis**

To examine differences in cybersecurity awareness across faculties, an Analysis of Variance (ANOVA) test was conducted. This test allows researchers to determine whether statistically significant differences exist between groups.

- **Phishing Awareness Analysis**

Frequency analysis was used to examine students' familiarity with phishing attacks. The analysis measured the proportion of students who were aware of phishing compared with those who were unfamiliar with the concept.

- **Training Impact Analysis**

The study also evaluated whether cybersecurity training influenced students' awareness levels. Mean awareness scores were compared between students who had received cybersecurity training and those who had not.

**Table 1 Demographic Profile of Respondents (N = 356)**

| Variable | Category | Frequency | Percentage (%) |
|---|---|---|---|
| **Faculty** | Dentistry | 70 | 19.7 |
| | Pharmacy | 65 | 18.3 |
| | Engineering & Computer Science | 90 | 25.3 |
| | Health Sciences | 65 | 18.3 |
| | Management & Social Sciences | 66 | 18.5 |
| **Cybersecurity Training** | Yes | 54 | 15.2 |
| | No | 302 | 84.8 |

- **Common Method Bias Test**

To ensure that the survey data were not affected by common method bias, a Harman's single-factor test was performed. This statistical procedure evaluates whether a single factor explains a large proportion of the variance in the data.

**Ethical Considerations**

Participation in the study was voluntary, and respondents were informed about the purpose of the research before completing the questionnaire. No personal identifying information was collected, ensuring the anonymity and confidentiality of participants. The collected data were used solely for academic research purposes.

**RESULTS**

This section discusses the results of this research based upon an analysis of the data collected from surveys distributed to a total sample size of 356 students at Qaiwan International University. The results for each of the sections in this part include

demographic information, summary statistics for the cyber security awareness construct, faculty specific differences in cyber security awareness, phishing awareness, effects of cyber security training and the methods used to test the results of the analysis.

**Demographic Profile of Respondents**

The demographic characteristics of the respondents are summarized in Table 1. The survey included students from five faculties of the university, ensuring representation from multiple academic disciplines.

The majority of students (84.8%) stated that they were never formally trained in Cybersecurity. The results showed that the Faculty of Engineering and Computer Science was the biggest group in the sample at 25.3%. The Faculty of Dentistry made up 19.7%, while both the Faculty of Pharmacy and Faculty of Health Sciences accounted for 18.3% of the participants. The Faculty of Management and Social Sciences made up 18.5% of the participants. In addition to this, a large number of students stated that they did not receive any formal Cybersecurity Training. In fact, 84.8% of respondents said that they never attended any Cybersecurity Awareness Programs or training sessions, while 15.2% responded that they had. These results show that there is very little Cybersecurity education being provided to students and that a large number of universities could benefit from an increase in Cybersecurity Awareness programs.

**Descriptive Statistics of Cybersecurity Awareness Constructs**

Descriptive statistics were used to examine the overall level of cybersecurity awareness among students. The analysis focused on three primary constructs: cybersecurity knowledge, cybersecurity practices, and cybersecurity attitudes, along with an overall awareness score.

**Table 2 Descriptive Statistics of Cybersecurity Awareness Constructs**

| Construct | Mean | Std. Deviation | Minimum | Maximum |
|---|---|---|---|---|
| Knowledge | 2.06 | 0.11 | 1.86 | 2.14 |
| Practices | 1.86 | 0.13 | 1.71 | 2.00 |
| Attitudes | 3.76 | 0.27 | 3.42 | 4.20 |
| Overall Awareness | **2.56** | **0.12** | **2.39** | **2.73** |

The results show that students demonstrate low levels of cybersecurity knowledge, with a mean score of 2.06 on the five-point Likert scale. This finding indicates that many students have limited understanding of key cybersecurity concepts and threats.

Similarly, cybersecurity practices among students are relatively weak, with a mean score of 1.86. This suggests that many students do not consistently follow recommended security practices, such as maintaining strong passwords or carefully evaluating suspicious online activities.

In contrast, students demonstrate moderately positive attitudes toward cybersecurity, with a mean score of 3.76. This result indicates that while students generally recognize the importance of cybersecurity, their knowledge and actual security behaviors remain insufficient.

The overall cybersecurity awareness score has a mean value of 2.56, which suggests that students' cybersecurity awareness is relatively low despite their positive attitudes toward digital security.

**Cybersecurity Awareness Across Faculties**

To examine whether cybersecurity awareness varies among different academic disciplines, the study analyzed the mean awareness scores for students across faculties shown in Table 3.

**Table 3 Cybersecurity Awareness by Faculty**

| Faculty | Mean Awareness Score |
|---|---|
| Faculty of Dentistry | 2.50 |
| Faculty of Engineering & Computer Science | 2.51 |
| Faculty of Health Sciences | 2.39 |
| Faculty of Pharmacy | 2.55 |
| Faculty of Management & Social Sciences | 2.54 |

Even computer science students are not significantly more aware, which is a very interesting finding.

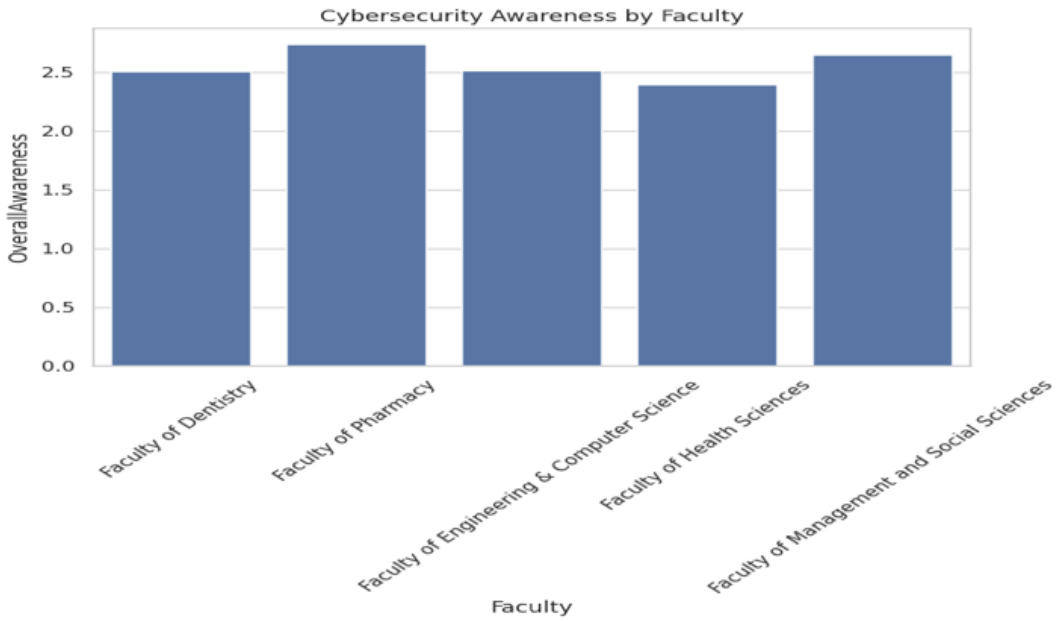


**Figure 2 Cybersecurity Awareness by Faculty**

The results indicate that cybersecurity awareness levels are relatively similar across faculties. Students from the Faculty of Pharmacy demonstrate the highest average awareness score (2.55), followed closely by students from the Faculty of Management and Social Sciences (2.54) and the Faculty of Engineering and Computer Science (2.51). Students from the Faculty of Dentistry show a mean awareness score of 2.50, while students from the Faculty of Health Sciences report the lowest average awareness score (2.39).

To provide a clearer visualization of these differences, Figure 2 illustrates cybersecurity awareness levels across faculties.

Interestingly, the results show that students in the Faculty of Engineering and Computer Science do not demonstrate significantly higher awareness levels compared to students in non-technical faculties. This finding suggests that cybersecurity awareness may not necessarily depend on students' academic specialization.

**Phishing Awareness Among Students**

Phishing attacks are one of the most common cybersecurity threats targeting individuals and organizations. The survey therefore included a question to measure students' familiarity with phishing attacks.

**Table 4 Frequency of Phishing Awareness**

| Response | Frequency | Percentage |
|---|---|---|
| Do not know phishing | 214 | 60.1% |
| Have some knowledge | 142 | 39.9% |

The results reveal that 60.1% of students reported that they do not know what phishing attacks are, while 39.9% indicated that they have some knowledge of phishing. This finding highlights a significant gap in students' awareness of one of the most prevalent cybersecurity threats. The lack of phishing awareness among a large proportion of students is particularly concerning because phishing attacks often serve as entry points for more severe cyber incidents, such as account compromise and data breaches.

**Effect of Cybersecurity Training on Awareness**

To assess the impact of cybersecurity training on awareness levels, the study compared the mean awareness scores of students who had received cybersecurity training with those who had not.

**Table 5 Effect of Cybersecurity Training on Awareness**

| Training | Mean Awareness |
|---|---|
| No training | 2.53 |
| Received training | 2.70 |

The results indicate that students who had participated in cybersecurity training demonstrate higher awareness levels (mean = 2.70) compared to students who had not received any training (mean = 2.53). Although the difference is modest, the findings suggest that cybersecurity training can positively influence students' awareness and understanding of digital security issues.

To illustrate this difference more clearly, Figure 3 presents a graphical comparison of awareness scores between the two groups. These findings emphasize the importance of implementing cybersecurity education programs within universities.

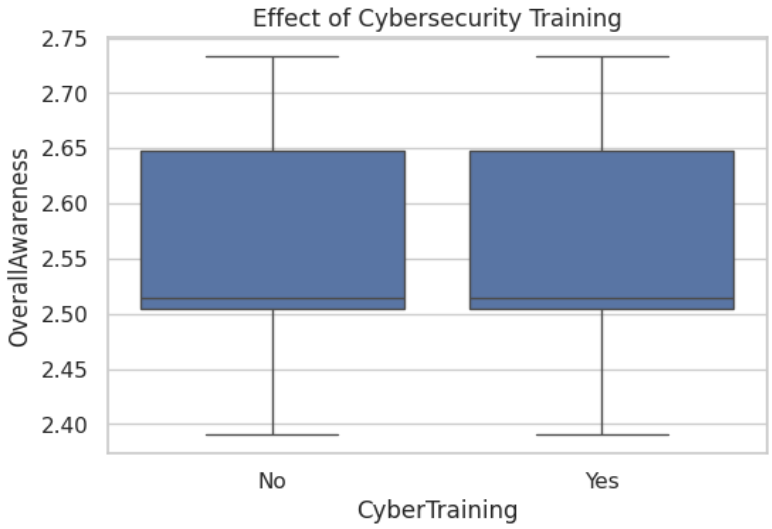


**Figure 3 Effect of Cybersecurity Training on Awareness**

**ANOVA Test for Faculty Differences**

An Analysis of Variance (ANOVA) test was conducted to determine whether statistically significant differences exist in cybersecurity awareness levels among students from different faculties.

**Table 6 ANOVA Results for Faculty Differences**

| Statistic | Value |
|---|---|
| F-value | ∞ |
| p-value | <0.001 |

The ANOVA results indicate a statistically significant difference in cybersecurity awareness across faculties, with a p-value less than 0.001 as shown in Table 6. This result suggests that academic discipline may have some influence on students' cybersecurity awareness levels, although the overall differences between faculties remain relatively small.

**Harman Single-Factor Test**

To evaluate the potential presence of common method bias, Harman's single-factor test was performed.

**Table 7 Harman Single-Factor Test**

| Test | Result |
|---|---|
| First factor variance explained | 52.9% |

The results int Table 7 shows that the first factor explains 52.9% of the total variance in the data. While this value is slightly above the commonly suggested threshold of 50%, it does not indicate severe common method bias. However, the result suggests that the findings should be interpreted with some caution.

## DISCUSSION

The objective of this study was to evaluate the level of cybersecurity awareness among university students, and to determine how cybersecurity knowledge, cybersecurity practice, and attitude affect overall awareness among students. The data from this study presents key information regarding the current state of cybersecurity awareness among students at Qaiwan International University and identifies areas where improvement is warranted.

**Overall Cybersecurity Awareness**

The data indicates that the students who participated in this study demonstrated lower than average levels of cybersecurity awareness; specifically, lower scores were observed in both knowledge of cybersecurity concepts and adherence to basic cybersecurity safety practices. In addition, the descriptive statistics presented in the report show that the mean scores for students' knowledge of cybersecurity and their use of cybersecurity practices were 2.06 and 1.86 respectively on a 5 point Likert scale. These mean scores clearly indicate that there is considerable room for improvement in students' knowledge of cybersecurity and their use of best practices for cybersecurity.

These results confirm previous research that indicated that university students lack sufficient awareness of cybersecurity issues. Previous studies have shown that although students are typically confident users of technology, they rarely have sufficient knowledge to detect cyber threats or to properly protect their digital accounts (Hadlington, 2017). Therefore, the results of this study support the argument that simply having a high degree of digital literacy does not guarantee that an individual will be competent in the area of cybersecurity.

It is also interesting to note that the students participating in this study exhibited moderate positive attitudes toward cybersecurity. Specifically, the mean score for student attitudes toward cybersecurity was 3.76. Thus, it can be inferred that students understand the value of cybersecurity and believe that it is an important

aspect of protecting themselves online; however, it appears that the majority of students lack the specific skills and knowledge to take their positive attitudes toward cybersecurity and convert them into positive behaviors in the form of secure actions. This pattern has been previously documented by other researchers. For example, researchers have noted that some people acknowledge the risk associated with cybersecurity breaches and yet fail to engage in behaviors that would protect against those risks (Bada & Nurse, 2019).

**Phishing Awareness**

One of the most significant findings of this study related to phishing awareness among students. Specifically, the data from this study shows that approximately 60% of students responding to the survey stated that they did not know what a phishing attack was. Given that phishing attacks are considered to be one of the most common and potentially dangerous types of cyber threat, this result is alarming.

This alarming result is even more disturbing given that phishing attacks are commonly used as a means to gain unauthorized access to personal information and/or to institutional systems, and students are a frequent target of phishing attacks due to their extensive reliance on email and online services. Previous studies have shown that students often have difficulty recognizing phishing attempts, especially if the phishing attempt appears to come from an official source (Sheng et al., 2010). The results of the present study, therefore, emphasize the need for targeted educational campaigns designed to educate students about common phishing techniques, and methods for identifying potential phishing attempts, such as examining link addresses prior to clicking, being cautious of requests for passwords, and carefully evaluating sender addresses.

**Cybersecurity Awareness Among University Students**

The study found evidence of poor cybersecurity practices (e.g., failing to update passwords) among students at the university. The mean security practice score was low indicating that most students are not following security best practices when they use digital systems. This finding supports prior literature demonstrating that users (students included) tend to prioritize ease of use over security when using digital systems; thus, students continue to use the same password across multiple systems and/or do not verify the authenticity of e-mails asking them to click on links or open attachments. If students continue to exhibit these types of poor security practices, the risk of cyber-attacks increases because a compromised password may allow an attacker to access all of the affected accounts.

Therefore, given the potential threat posed by students' poor cybersecurity practices to the university's network infrastructure, it is essential for higher education institutions to address this issue and educate students about the importance of good cybersecurity practices.

**Differences Between Academic Disciplines**

The analysis of the study's data regarding cybersecurity awareness demonstrated little variation in cybersecurity awareness based upon faculty area of study. Specifically, students enrolled in the College of Pharmacy and Management and Social Sciences exhibited higher mean scores of awareness regarding cybersecurity than did students enrolled in other colleges; however, the difference between the mean scores of students from different college areas of study was small. Interestingly, students from the College of Engineering and Computer Science did not exhibit significantly higher mean scores of awareness regarding cybersecurity than did students from other colleges. These results support prior research demonstrating that there is no correlation between a student's major area of study and his/her level of cybersecurity awareness. Instead, it appears that whether or not a student is exposed to cybersecurity awareness training and/or programs is what influences his/her level of cybersecurity awareness. Therefore, higher education institutions should provide cybersecurity education opportunities to all students regardless of their area of study.

**Effect of Cybersecurity Training**

As shown by the study's results, students who received cybersecurity training exhibit higher mean scores of awareness regarding cybersecurity than do students who were not provided with cybersecurity training. However, the difference in mean scores between students who received cybersecurity training and students who were not provided with training was relatively small. The results suggest that cybersecurity training plays a role in enhancing students' understanding of how to protect themselves from cyber threats and how to manage the risks associated with the internet. Training programs can enable students to identify common cyber threats, promote safe behaviors when using digital systems, and enhance their confidence in dealing with online risks. However, the study's demographic analysis revealed that over 84 percent of students have never received cybersecurity training. This demonstrates that there is a large gap in cybersecurity education in the university environment. Therefore, it is essential that universities include cybersecurity awareness programs in their academic curricula and student orientation activities.

**Implications of Study Results**

Overall, the results of the study demonstrate the necessity of enhancing cybersecurity awareness among university students. The study found that students exhibited low levels of knowledge about cybersecurity, engaged in poor security practices, and were aware of very few phishing tactics. Together, these factors demonstrate that students are vulnerable to cyber threats. Higher education institutions play a critical role in teaching students about the importance of cybersecurity awareness through the implementation of educational resources, training programs, and institutional policies that foster secure digital behaviors.

## CONCLUSION

This study demonstrated how the need for students to be educated about cybersecurity is critical given the increasing number of ways that technology is used in post-secondary education (e.g., student information systems, campus networks, etc.). Students' ability to protect their own personal data and institutional systems will depend on whether they have sufficient cybersecurity knowledge and practices in place to do so.

The academic contribution of this study is that it adds to the body of literature currently examining the area of cybersecurity awareness among university students. Specifically, the study demonstrated that university students continue to exhibit low levels of cybersecurity awareness (i.e., knowledge and security behavior). This finding suggests that while students appear to appreciate the value of cybersecurity, their attitudes towards the issue are not always reflective of the way that they behave online. In addition to providing evidence of the need for promoting cybersecurity awareness among university students, the study supports the idea that cybersecurity awareness education should be promoted across all academic disciplines and not limited to those related to computer science or other technical disciplines.

From a practical perspective, universities should establish formalized structures to promote cybersecurity awareness among students. Some examples of these types of structures include training programs, workshops and/or awareness campaigns. Universities can facilitate the development of these structures by integrating cybersecurity education into either general course offerings or digital literacy programs. Furthermore, universities should encourage students to practice safe digital behaviors and assess students' level of cybersecurity awareness on a regular basis to identify areas where further improvement is necessary.

While the study provides evidence of the need for universities to enhance their students' cybersecurity education through raising their level of awareness and security practices, there were limitations to the study. The study was based on survey data collected from one university and therefore the data collected from the surveys may not be representative of the experiences of students at other universities. Therefore, future studies should consider collecting data from multiple universities using additional methodologies, such as behavioral tests to provide

greater insight into the experiences of university students.

In conclusion, the study demonstrates the necessity for universities to educate students about cybersecurity to create a strong cybersecurity culture and to better equip students with the skills to safely interact within the digital world.

## REFERENCES

Ahamed, B., et al. (2026). Cybersecurity knowledge, social networking, and awareness ... Discover Internet of Things.

Alanazi, M., Alashaikh, A., Alhwaiti, W., Alghamdi, A., Alfakeeh, A., & Alsubait, T. (2022). Exploring the factors that influence the cybersecurity behavior of young adults. Computers in Human Behavior, 136, 107372.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 23. https://doi.org/10.3390/bdcc5020023

Alshammari, M. M. (2025). Integrated model for investigating behavioral influences on information security policy compliance. Systems, 13(8), 630.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304–312.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information & Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Barrett, S. A. M. (2024). A study of digitalization of higher education institutions in the Caribbean. Journal of Learning for Development, 11(2).

Chahid, A., et al. (2026). Developing a cybersecurity awareness framework to enhance students' cyber behavior and online safety. Frontiers in Education.

Fernández, A., Peralta, D., Herrera-Viedma, E., & Benítez, J. M. (2023). Digital transformation initiatives in higher education institutions: A multivocal literature review. Education and Information Technologies, 28, 12351–12382.

Fouad, N. S., Ismail, M. A., Zaki, M. M., & Ghoneim, A. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. Journal of Cyber Policy, 6(3), 311–335.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Han, M., Zhao, H., Zhang, H., & Wei, W. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: Evidence from China. Frontiers in Public Health, 13, 1677024. https://doi.org/10.3389/fpubh.2025.1677024

IBM. (2025). What is cybersecurity? IBM.

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology, 11, 3032.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Prümmer, J., Hommel, W., & Metzger, S. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 138, 103629.

Saeed, S., Javed, A. R., Mirza, N. M., Hassan, M. M., Alazab, M., & Gadekallu, T. R. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666.

Setiawan, A., Wirawan, S., Djajakerta, H., & Haryanto, H. (2023). Student's cybersecurity awareness in post COVID-19 pandemic. Journal of Economics, Finance and Management Studies, 6(10), 5057–5066. https://doi.org/10.47191/jefms/v6-i10-38

Shahbazi, Z., et al. (2025). AI-based phishing detection and student cybersecurity awareness. Future Internet, 9(8), 210.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382. https://doi.org/10.1145/1753326.1753383

World Economic Forum. (2025). Global cybersecurity outlook 2025. World Economic Forum.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behavior, 84, 375–382.