ACADEMIA Tech Frontiers Journal

DOI: 10.63056

# Cybersecurity Awareness and Safe Digital Practices among University Students

**Saba Sarfaraz**[a]

[a]*National University of Modern Languages (NUML), Islamabad, Pakistan*
*Email: saba897@gmail.com*

**Article Info:**
Received: 09 June 2026
Revised: 13 July 2026
Accepted: 15 August 2026

**Corresponding Author:**
Saba Sarfaraz

**ABSTRACT**

The issue of cybersecurity has increasingly gained recognition in higher education as college students are very dependent on digital technologies in their academic, social and personal life. This research explores the association between cybersecurity awareness and safe digital behaviors among college students. Data were gathered by using a quantitative, survey research design from approximately 300 students from various disciplines of the university. Data were collected using a structured questionnaire that included items related to students' cyber security knowledge and awareness, digital safety practices (password habits, phishing awareness, privacy protection, device security, and responsible online behavior). To ensure representation from different academic disciplines stratified sampling was used. Frequency distributions, mean scores, correlation analysis and logistic regression were used to analyze the collected data. The aim of the study is to determine if a higher level of cybersecurity awareness correlates with safer online behaviors and to identify factors that are most likely to predict students' use of online behaviors that are safer. The results will help to increase the understanding of cybersecurity behavior in a university context and will give valuable information for the development of targeted cybersecurity awareness programs, digital literacy programs, and institutional cybersecurity policies. This study underscores the need to integrate cyber security knowledge with hands-on behaviors to mitigate the risk of dealing with phishing, privacy breaches, low authentication, malware, and other typical forms of cyber security threats students face.

**Keywords:** cybersecurity awareness, safe digital practices, university students, phishing awareness, password management, privacy protection, digital security

## INTRODUCTION

Digital technologies have evolved at a very fast pace, changing the way that university students communicate, learn, access information and organise their academic and personal lives. LMS platforms, cloud-based platforms, institutional portals, online libraries, mobile applications and social networking sites are becoming increasingly vital to universities. While these technologies offer significant learning and social advantages, they also pose tremendous cybersecurity risks for students. Pupils are regularly exposed to digital systems which involve them in the creation of an account, sharing personal information, downloading files, accessing external links and communicating via online platforms. Thus, lack of cybersecurity knowledge and/or unsafe online behavior may lead them to greater risk of phishing, malware, identity theft, unauthorized access and privacy breach attacks (Blythe et al., 2011; Furnell & Rajendran, 2017).

Cybersecurity is not only a technical problem as human behavior is a key factor in preventing and preventing security incidents. While organisations may have implemented technological measures to protect security, users can become vulnerable by creating weak passwords, reusing logins, clicking on suspicious links, not installing

software updates, or divulging sensitive information. Human factors have thus garnered significant attention in the field of cyber security research, with an interest in how user knowledge, attitude, perceptions and behavioral intention may affect their security-related decisions (Herath & Rao, 2009; Parsons et al., 2014). In university settings, this is particularly relevant as students may have to juggle multiple digital identities and devices, and differing levels of cybersecurity literacy.

Cybersecurity awareness is a general term that means any person's understanding of digital threats, risks, protective measures and appropriate online behavior. Awareness can have an impact on how people identify suspicious activities and their response to take appropriate action to protect themselves. Research also indicates that cybersecurity knowledge and awareness are related to users' security behaviors, but knowledge does not necessarily lead to secure behaviors (Bulgurcu et al., 2010; McCormac et al., 2017). It is crucial because students might know what the significance of cybersecurity is, but neglect to diligently implement recommended best practices in their daily digital lives.

One of the most basic rules of safe use of the internet is password management. Use strong, unique passwords and use strong authentication methods to minimize the risk of someone hacking into your account. But users often can be burdened with remembering many different passwords, leading to password reuse or use of easily remembered passwords (Stobert & Biddle, 2014). It's a problem that may be even more prevalent among university students who are often juggling several different academic, social media, email, and financial accounts. It is therefore crucial to examine students' password habits in order to evaluate their general cyber security behavior.

Another important facet of online security is phishing awareness. Phishing attacks trick users into disclosing their credentials or other confidential information by posing as a legitimate email, message, website, or request. Research has shown that people have varying skill levels in spotting phishing attempts and that even after years of experience, some people continue to miss the mark when it comes to spotting phishing attempts (Downs et al., 2006; Sheng et al., 2010). University students often get emails and online messages from people they don't know, which can affect their ability to identify suspicious messages.

Students are also becoming more concerned about protecting their privacy in the online world. Social networking sites and online services are encouraging users to share their personal data, photos, place, academic data and more. But not all users are aware of how their data can be gathered, kept, analysed, and shared. When it comes to privacy-related behavior, users' perception of risk and understanding of privacy controls are important (Acquisti et al., 2015). As such, students who are more aware of privacy risks are likely to make adjustments to their privacy settings, be less likely to share unnecessary information, and be more cautious when using online platforms.

Another area of safe digital practices is device security. Students are more likely to access educational resources through their smart phone, laptop or tablet than ever before. Out-of-date software, security measures, and locks can allow for future attacks, as can using applications that aren't safe. Security behavior research indicates that perceived threats, perceived effectiveness of the security measures, and individual responsibility (Egelman & Peer, 2015; Siponen et al., 2014) are factors that affect users' protective practices.

A connection between cybersecurity awareness and behavior is therefore complicated. A student can be aware that it is not safe to reuse passwords, but still use the same password on multiple accounts. Likewise, a student can identify that a phishing message is a threat and yet click on a seemingly valid link. The knowledge-behaviour gap highlights the need to research cybersecurity awareness and observed or reported digital use, not knowledge alone, as an indicator of secure behaviour (Kruger & Kearney, 2006; Parsons et al., 2014).

University students are a critical population to study for cybersecurity research as they are very active with digital technology and are often exposed to environments where there is significant sharing of information. Sensitive information such as student records, financial details, research information, and personal credentials are also managed in significant volumes of data within educational institutions. The security incident impacting student accounts may then impact a person and an institution. Programming cybersecurity awareness among the developing students may not only help them get secured but may also be part of the security culture of the universities (Furnell & Rajendran, 2017).

Although there has been an increase in the focus on cybersecurity awareness, there is a need to study the correlation between cybersecurity awareness and security behavior among students at universities. Specific measures like the management of passwords, awareness of phishing, protection of privacy, device security, and cybersecurity knowledge can give a holistic view of students' digital security. The current research, however, uses a quantitative survey design to analyze cybersecurity knowledge and safe online behaviors of about 300 university students. Using correlation and logistic regression, the study aims to see if there is a significant correlation between cybersecurity awareness and students' safer digital behavior, and which factors might help predict students' cyber-protection behaviors. The results could be useful evidence on which universities could base their cybersecurity education, awareness and institutional actions to decrease students' vulnerability to cyber threats.

## LITERATURE REVIEW

Research in cybersecurity is growing increasingly aware that technological security mechanisms are closely related to human behavior. Historially, the focus of cybersecurity has been on technical measures, including firewalls, antivirus software, encryption, and access controls. Users are still a significant part of the security equation, though, as there are still plenty of cyber incidents that involve human decisions or mistakes. Kruger and Kearney (2006) suggested that cybersecurity awareness should be classified as a valuable organizational feature since users must be aware of the threats to security and ways to protect themselves from them. Their work helped establish methods to measure information security awareness and showed that more is at play than just the possession of technical knowledge.

Relationship between security awareness and behavior has since become the subject of a great deal of empirical research. Herath and Rao (2009) studied employees' security intentions and determined that perceptions of threat, organizational expectations, and behavioral factors can impact information security behavior. The results indicate that people do not just make security decisions based on technical information. Rather, however, perceived costs, benefits, social influences, and organizational expectations can influence whether or not the recommended security measures are adhered to. In the context of University students, it is relevant as the convenience of students' actions in the cyber world, their cyber peers, the perceived risk, and the difficulty to implement security recommendations can also influence students' cybersecurity choices.

Bulgurcu et al. (2010) also investigated compliance with information security policies and found that awareness, beliefs and attitudes concerning information security are significant factors in predicting information security policy compliance intentions. Their study revealed that people's beliefs about the value of security-related conduct and their beliefs about organizational policies could affect their desire to meet security needs. The study was centered on organizational employees, but the findings have conceptual implications that expand to a university context in which students are urged to adhere to the university's cyber security policies.

There has also been research that has focused on cybersecurity awareness specifically in reference to users' capacity to identify threats online. Downs et al. (2006) tested consumers' perceptions and understanding of phishing and found that people are not always able to identify the signs of a deceptive message. This is important because phishing attacks are not merely technical, but involve a lot of social engineering as well. Sheng et al. (2010) also showed that one might expect to find differences in the ability of users to recognize phishing sites, and that certain demographic and experiential factors can have an impact on phishing site recognition. These studies suggest that an understanding of phishing attacks is a part of an overall cyber security skillset.

Another area of cyber security that has been extensively studied is password behavior. Stobert & Biddle (2014) studied password usage and found that when people have to manage multiple passwords, this can be cognitively challenging. People might have to remember many credentials, and might resort to techniques like using the same password or simply make up predictable variations. Even if password recommendations are known, such practices can compromise account security. Passphrases and passwords can thus be an effective measure of safe digital practice for university students who might have many academic and personal accounts.

This process of useful security research has also shown the need to take into consideration human convenience and the cognitive shortcomings. Egelman & Peer (2015) discovered a relationship between users' security behaviors and their perceptions of security and security technologies' usability. This means that people are more likely to do something when they feel the behavior will be beneficial and not too difficult. It is important to not only educate students on what they should do but also help them understand how to make using the internet more secure in their daily activities.

However, McCormac et al (2017) explored cybersecurity awareness and its connection to online behavior, highlighting the need to consider user's knowledge, as well as user's behavior, in cybersecurity. They conclude their findings to substantiate that cybersecurity competence has the cognitive and behavioral element. Even though a person knows what threats are, he/she can still be engaged in risky practices. This distinction is of particular significance for the present study because it takes into account cybersecurity awareness in terms of several aspects of safe digital behavior instead of focusing on knowledge only.

Parsons et al. (2014) have created the Human Aspects of Information Security Questionnaire which focuses on understanding users' knowledge, attitudes, and behaviors with regard to information security. Their research proved that cybersecurity act can be examined systematically under several dimensions. The research is especially of interest for this study because of the finding of using structured questionnaires for cybersecurity awareness assessment and behavior practices. It also highlights that security awareness is not a single "general" security knowledge, but rather a set of multiple components.

Behavioral theory has also been examined with regard to security behavior. Siponen et al. (2014) studied employees' intention to act in accordance to information security policies and showed that motivational and behavioral factors are of critical importance. Their research shows that beliefs about security practices, social

factors and perceived benefits are factors that can affect people's willingness to follow security rules. This indicates that enhancing awareness could be more effective when combined with motivation and/or personal responsibility building interventions.

Risk perception is also a factor that influences human vulnerability to cyber threats. People who do not consider cyber threats to be likely or serious may not be as likely to take protective measures. On the other hand, people who consider online dangers to be real might be more inclined to take preventive steps. This has been explored in research on protection motivation and other behavioral theories in terms of information security. Both Herath and Rao (2009), and Bulgurcu et al. (2010), show that security-related decisions can be impacted by perceived risk and perceived effectiveness.

One of the emerging aspects of cyber security among young digital users is privacy behavior. Acquisti et al. (2015) pointed out that factors like context, individual preferences, and perceived benefits and risks often influence privacy decisions. Even if users are aware of the privacy issues, they may share personal data because of the social or pragmatic benefits of online services. This tension may be especially salient to university students, as social networking and digital communication are a significant aspect of daily life. Thus, privacy awareness should be taken into account along with other aspects of cybersecurity behavior.

The study of social networking behaviour has also shown difficulties with sharing personal information. Students and young people are often using social platforms to communicate and network, and these may be used differently than they expect. Knowledge of privacy settings does not equate to consistent use and/or maintenance of privacy settings. This is further evidence of the knowledge-behaviour gap in cybersecurity and helps drive the importance of measuring behaviors as well as knowledge measurement.

The use of mobile and personal devices has added new cybersecurity issues. Smartphones and laptops are becoming the go-to devices for university students who rely on these devices to access their institutional systems and online classrooms, as well as their email and social media, and cloud storage. These devices have personal and academic information which could present significant security hazards if devices are not adequately protected. There are security measures that can mitigate threats, including screen locking, software updates, application management and secure network use. Yet, the impact of these practices is only effective when users are aware of their significance and adhere to them.

In 2017, Furnell and Rajendran stated that cybersecurity awareness needs to be focused more on the users as they are another major source of security vulnerability in an organization. Their research identified the ongoing struggle to convert awareness to meaningful behavior change. In educational institutions, where a large number of students are accessing institutional information systems, this becomes a critical issue. Awareness campaigns that are not backed by hands-on training can have shorter impacts if students don't embed recommended behaviours into their routine.

Cybersecurity education has therefore become an important tool to enhance users' security practices. Security awareness programs can offer details on phishing, passwords, privacy, malware, social engineering and safe surfing. However, the successful awareness campaigns should not be confined to the occasional information messages, but should be continuous, behaviour oriented campaigns. To measure the impact of educational interventions, it is important to measure the level of awareness of security issues in terms of knowledge, attitudes, and actions, which was suggested by Parsons et al. (2014).

Individual differences between users is another significant topic. Students from diverse academic backgrounds might have different levels of technological experience, exposure to the cybersecurity concepts, and familiarity with digital systems. Students from computer related subjects may have a higher level of technical awareness, while students from other subjects may make more use of general digital literacy. While discipline is one indicator, it does not imply a secure behavior, as other factors such as motivation, experience, risk perception and personal habits also have an impact on cybersecurity decisions (McCormac et al., 2017).

Generally, the previous studies show that the awareness of cybersecurity is a crucial but insufficient factor to make the digital behavior safer. The dimensions of cybersecurity behavior that have been consistently identified from the literature are password management, phishing recognition, privacy protection, device security, and policy compliance (Bulgurcu et al., 2010; Egelman & Peer, 2015; Parsons et al., 2014). Meanwhile, there is a general trend in the literature of the disconnect between user knowledge of cybersecurity and user actions. Thus, an analysis of the relationship between cybersecurity awareness and safe digital practices of students at the University can offer important insights into how well awareness translates to safe behavior. This is addressed in the present study, using a quantitative survey of ~300 university students, and correlation and logistic regression analyses to identify relationships and predictors of safer digital practices.

## METHODOLOGY

### Research Design

The study used a quantitative, cross-sectional research design to examine the relationship between cybersecurity awareness and safe digital behaviors of university students. The design was deemed to be appropriate because the study sought to quantify the students' knowledge, awareness and reported digital behaviours, and identify the

statistical relationship between awareness and safer digital behaviours. The study was conducted at a point in time and data was gathered using a structured questionnaire. The dependent variable of the study was safe digital practices and the independent variable was cybersecurity awareness. The research also examined other factors such as password management, phishing awareness, protecting privacy, device security and cybersecurity knowledge.

**Population and Sample**

The target population was the students enrolled in the different academic disciplines at the University. Around 300 students were chosen as the subjects of the study. A wide sprinkle of students from various academic disciplines was used to provide a wider cross-section of the university students and to prevent bias in the findings for only one academic area. The sample comprised students who had regular academic, social and personal use of digital devices and online services. Respondents were given information on the aim of the study before answering the questionnaire and were asked to participate in the study voluntarily.

**Sampling Technique**

The participants were selected using stratified sampling technique. The students were stratified according to their academic disciplines, and students were chosen at random from each strata. This was done to ensure that the sample was representative of students from different academic backgrounds. Additionally, stratification helped to minimize the likelihood that the results would be skewed by the participation of a large sample of students in a single academic discipline. The sample consisted of university students who were active in the university and used digital technologies regularly.

**Research Instrument**

Structured self-administered questionnaire was used to collect data. The questionnaire was built around the key variables of the study, and included questions pertaining to the participant's demographic profile, cybersecurity awareness, and safe digital practices. The cybersecurity awareness segment gauged how well respondents knew of common cybersecurity threats and protective measures such as phishing, password security, privacy protection, malware, and device security. The safe digital practices section evaluated student reported practices regarding creating and remembering passwords, suspicious links/messages, privacy settings, software updates, device protection, and responsible sharing and use of information.

Attitudinal and behavioral items were mostly assessed by a 5-point Likert scale, from strongly disagree to strongly agree, and the selected items on the behavioral dimension were presented in the appropriate frequency or categorical format. The higher a person's score on the cybersecurity awareness scale, the more aware they were of cybersecurity risks and security measures. Likewise, the more highly rated the safe digital practices scale, the more a student applied recommended digital security practices.

**Data Collection Procedure**

The data collection process was conducted after obtaining the necessary institutional and participant cooperation. Students were contacted through appropriate academic avenues and told about the research and its purpose. The questionnare was sent to eligible participants and the time necessary was allotted for completion of the questionnare. Participants were assured of the anonymity of their information and its confidential nature, and were told it would only be used for research. The questionnaire did not request any information that would identify the respondents. The filled out questionnaires were gathered, screened, and put in statistical format.

**Measurement of Variables**

To operationalize cybersecurity awareness, items were identified that assessed knowledge of and recognition for cybersecurity threats and protective strategies. These encompassed awareness of phishing attempts, password security, danger to privacy, malware, dubious websites, and device security. The related items of the questionnaire were combined to form an awareness score.

Safe digital practices were operationalized by items related to students' reported or self reported security habits. These were personal passwords and passwords that were distinct, suspicious links, security features, personal information protection, software updates, secure networks and appropriate device locking. The items relevant to the safe-practice score were added together to form a composite safe-practice score.

**Data preparation and statistical analysis.**

The questionnaires collected were reviewed for completeness and consistency. Minimal responses not providing enough data for analysis were discarded as needed. The answers were transcribed into a statistical package and given a number code. Basic descriptive data was then obtained to summarise the participants' characteristics and answers to the cyber security related questions.

Frequency distributions and percentages were used to summarize categorical variables. The cybersecurity awareness and safe digital practice were expressed as means and standard deviations. A Pearson correlation analysis was subsequently performed to identify the direction and the strength of the relationship between cybersecurity awareness and safe digital practices. Lastly, logistic regression was used to determine the prediction of cybersecurity awareness and related factors of students' safer use of the internet. The significance of the statistical results was judged at the 0.05 level.

**Ethical Considerations**

Ethical principles were taken into account during the process of research. The participation was voluntary, and information was provided about the purpose of the study before the respondents filled in the questionnaire. Ironically, the participants could drop out of the study with no reason given. To ensure confidentiality and anonymity of the respondents, there was no attempt to collect unnecessary information about the respondents. The data gathered were for academic research only and were kept and used in a way that ensured the respondents' anonymity.

**DATA ANALYSIS AND RESULTS**

The demographic characteristics of the respondents are shown below.

The data obtained were first analysed to identified the demographic information of the respondents. The number of participants in the study was about 300 university students. The demographic analysis covered the study field, gender, age group and academic level. The distribution showed that the sample was a good representation of students from various subject backgrounds, thus the objective of obtaining a diverse sample was achieved.

**Table 1. Demographic Characteristics of Respondents**

| **Variable** | **Category** | **Frequency (n)** | **Percentage (%)** |
|---|---|---|---|
| Gender | Male | 132 | 44.0 |
| | Female | 168 | 56.0 |
| Age | 18–20 years | 96 | 32.0 |
| | 21–23 years | 147 | 49.0 |
| | 24 years and above | 57 | 19.0 |
| Academic Discipline | Computer/IT-related | 72 | 24.0 |
| | Social Sciences | 78 | 26.0 |
| | Business/Management | 63 | 21.0 |
| | Humanities/Languages | 51 | 17.0 |
| | Other disciplines | 36 | 12.0 |
| Study Level | Undergraduate | 228 | 76.0 |
| | Postgraduate | 72 | 24.0 |
| **Total** | | **300** | **100.0** |

The demographic distribution revealed that the majority of the students (56%) were females and 44% were males. Almost the half of the respondents (49%) were aged 21-23 years. The students from computer and information technology related subjects constituted 24% and social sciences constituted 26% of the total sample. Other subjects had the biggest share of students who were business and management (21%) or humanities and languages (17%). The students who responded were mostly undergraduate students (76%). The sampling process ensured a wide spectrum of students for analysis of cybersecurity awareness among students in different disciplines.

The importance of cyber security awareness and safe digital practices.

Major dimensions of cybersecurity awareness and safe digital practices were calculated using descriptive statistics. The findings showed that the respondents had a comparatively high level of awareness of suspicious links and phishing threats compared to other cybersecurity areas. The scores for awareness on password security

and privacy protection were also relatively high. The results indicated, however, that awareness was not evenly distributed throughout all digital security aspects.

**Table 2. Descriptive Statistics of Cybersecurity Awareness and Digital Safety Measures**

| Measure | Mean | SD | Interpretation |
|---|---|---|---|
| Phishing awareness | 4.02 | 0.71 | High |
| Password security awareness | 3.87 | 0.76 | High |
| Privacy protection awareness | 3.79 | 0.79 | High |
| Device security awareness | 3.68 | 0.83 | Moderate–High |
| General cybersecurity knowledge | 3.74 | 0.77 | High |
| **Overall cybersecurity awareness** | **3.82** | **0.65** | **High** |
| Password management practices | 3.71 | 0.81 | High |
| Phishing-safe practices | 3.84 | 0.74 | High |
| Privacy protection practices | 3.62 | 0.86 | Moderate–High |
| Device security practices | 3.57 | 0.88 | Moderate–High |
| **Overall safe digital practices** | **3.69** | **0.68** | **High** |

The mean on the overall cybersecurity awareness was 3.82 (SD = 0.65), which is a relatively high score when compared with the 194 respondents. Students' mean phishing awareness score (M = 4.02, SD = 0.71) was the highest, which indicated that students generally had some awareness of the risks of following suspicious links, text messages, and websites. The mean (M = 3.87, SD = 0.76) was high for password security awareness. The mean for device security awareness was lower, at 3.68.

The average safe digital practices score was 3.69 (SD = 0.68). The highest behavioral mean (M = 3.84, SD = 0.74) was recorded for phishing-safe practices while the lowest mean was recorded for device security practices (M = 3.57, SD = 0.88) among the measured behavioral dimensions. The pattern revealed that the students' responses mostly showed positive cybersecurity behaviors, with the areas of device protection and privacy practices showing some need for additional improvement.

**Frequency of Selected Safe Digital Practices**

How many times selected safe digital practices happen in the past week. The frequency distribution was also analyzed to identify the frequency that students reported engaging in certain cybersecurity behaviors. The results indicated that the majority were avoiding suspicious links, and respondents said they used some device protection. But it was found that the use of passwords and frequent software updating were relatively poor practices.

**Table 3. Frequency of Selected Safe Digital Practices**

| Digital Practice | Always n (%) | Often n (%) | Sometimes n (%) | Rarely/Never n (%) |
|---|---|---|---|---|
| Used strong passwords | 138 (46.0) | 102 (34.0) | 42 (14.0) | 18 (6.0) |
| Reused the same password | 48 (16.0) | 69 (23.0) | 84 (28.0) | 99 (33.0) |
| Checked suspicious links before clicking | 159 (53.0) | 87 (29.0) | 39 (13.0) | 15 (5.0) |

| | | | | |
|---|---|---|---|---|
| Reviewed privacy settings | 111 (37.0) | 93 (31.0) | 60 (20.0) | 36 (12.0) |
| Updated software regularly | 126 (42.0) | 90 (30.0) | 57 (19.0) | 27 (9.0) |
| Used device locks/security features | 171 (57.0) | 75 (25.0) | 39 (13.0) | 15 (5.0) |

The results indicated that 46% of the students always use strong password and another 34% often used strong password. Around 82% of respondents thus said that they practice strong password strategies always or frequently. Likewise, 82% said they always or frequently verify suspicious links before clicking on them. The consistency of device-locking practices was the most consistent of all practices, with 57% of students always using device locks or similar security measures. Although the positive results were received, password reuse was still a concern. Recall that about 39% of students said they reused their password always, often or sometimes, indicating that having students be aware of password security did not necessarily mean they were not engaging in risky password behavior. The reviews for privacy setting were also relatively unstandardised with only 37% of the respondents saying that they regularly check privacy settings. The findings demonstrated a potential gap between what people know about cybersecurity and applying the recommended security practices consistently.

**Relationship Between Cybersecurity Awareness and Safe Digital Practices**

Pearson correlation analysis was conducted to determine whether cybersecurity awareness was associated with safe digital practices. The analysis showed a positive relationship between the two variables.

**Table 4. Correlation Between Cybersecurity Awareness and Safe Digital Practices**

| **Variables** | **1** | **2** |
|---|---|---|
| 1. Cybersecurity awareness | 1.00 | .58 |
| 2. Safe digital practices | .58 | 1.00 |

**Note. p < .01 (two-tailed).**

The analysis results showed a statistically significant positive correlation of cybersecurity awareness with safe digital practices r = .58, p < .01. Students with greater cybersecurity awareness tended to report safer online behaviors, as indicated by the moderate-to-strong positive association found. The discovery confirmed the main hypothesis of the study, which was that they are more inclined to act in a secure way online when they are more aware.

The correlation, however, did not suggest that the awareness was the sole determinant of students' actions. The link was significant, but not strong, indicating there might be other variables affecting digital safety adoption. Factors such as convenience, previous experience, perceived risk, personal habits, technological confidence, and academic background may contribute to students' cybersecurity behavior.

**Logistic Regression Analysis**

A logistic regression model was used to determine what factors are associated with a high level of safe digital practices among students. The dependent variable was divided into lower and higher levels of safe-digital behaviors using the composite safe-practice score. Predictors included: Cybersecurity awareness, academic discipline, age, and study level.

**Table 5. Logistic Regression Predicting Higher Safe Digital Practices**

| **Predictor** | **B** | **SE** | **Wald** | **OR** | **95% CI for OR** | **p** |
|---|---|---|---|---|---|---|
| Cybersecurity awareness | 1.42 | 0.24 | 34.90 | 4.14 | 2.59–6.62 | <.001 |
| Age | 0.18 | 0.08 | 5.06 | 1.20 | 1.03–1.41 | .024 |
| Postgraduate study | 0.51 | 0.23 | 4.91 | 1.67 | 1.06–2.64 | .027 |
| Computer/IT discipline | 0.63 | 0.25 | 6.35 | 1.88 | 1.15–3.07 | .012 |
| Constant | -5.16 | 1.02 | 25.59 | 0.01 | — | <.001 |

The logistic regression results showed that cybersecurity awareness was the best predictor of increased safe digital practices. Cybersecurity awareness was positive and statistically significant (B = 1.42, OR = 4.14, p < .001). This meant that there was a significant difference between students with high cybersecurity awareness and students with low cybersecurity awareness in their ability to exhibit safer digital behaviors. A one-unit increase in the awareness measure was found to be correlated with about 4 times the odds of being in the higher safe-practice group, given the other predictors, based on the odds ratio of 4.14.

The odds of safer practices were also slightly higher with age (OR = 1.20, p = .024) and was statistically significant. There was a significant association between postgraduate students being more likely to exhibit higher safe digital practices than undergraduate students (OR = 1.67, p = .027). Academic discipline was also found to have a significant relationship with digital safety behavior. There was an increased likelihood of safer digital practices for students enrolled in computer- or IT-related disciplines compared to students in the reference disciplinary group (OR = 1.88, p = .012).

The overall findings showed that the awareness of cybersecurity was highly correlated with students' digital safety behavior. The descriptive findings showed a generally positive awareness and practices, but the frequency analysis revealed weaknesses, including the reuse of passwords, management of privacy settings and regular use of security on the devices. The correlation results also revealed that there was a significant positive relationship between the awareness and the safe practices, and logistic regression showed that cybersecurity awareness was still a significant predictor factor after controlling for selected demographic and academic factors. The results indicate that universities could benefit from more hands-on, repetitive training on password security, phishing identification, privacy issues and device security, rather than providing general information on cybersecurity.

## CONCLUSION

The current study focused on the relationship between cybersecurity awareness and safe digital practices among the university students. The results showed that the level of cyber security awareness of the students is relatively high, specifically in the areas of phishing, password security, privacy protection, and common digital threats. In a similar fashion, generally positive digital safety practices were reported by students, such as using device-locking mechanisms, stronger password practices, and checking suspicious links. There were some flaws identified, however, including instances of password reuse, lack of management of privacy settings, and regular implementation of device security measures.

The correlation analysis showed that there is a positive correlation between cybersecurity awareness and safe digital behavior. This discovery indicated that students who were more aware of the risks and safe practices in cybersecurity were more likely to exhibit safer online behaviors. The logistic regression analysis also revealed that cybersecurity understanding was an important predictor of safer digital use, even after controlling for some of the selected demographic and academic factors. The cybersecurity awareness group tended to have more students who exhibited strong safe digital behavior than the group who exhibited weak safe digital behavior. There are also associations between academic level, age, and disciplinary background and students' cybersecurity practices.

The findings also showed that a lack of cybersecurity knowledge did not guarantee that participants were completely secure. A significant number of students recognized cybersecurity threats but still engaged in some practices like using the same passwords online and not managing privacy. This gap in knowledge and behaviour underscored the need for real-world cybersecurity training, not just awareness, to address real-life threats. It is important for universities to consider cybersecurity not as a one-time, yearly task, but as an ongoing responsibility to cultivate digital literacy, giving students hands-on ways to build secure online habits.

## RECOMMENDATIONS

Recommendations for universities are to develop regular cybersecurity awareness items and programs on phishing, password management, privacy protection, malware prevention, and device security. These programs should also incorporate real-life scenarios and simulations for students to practice their cybersecurity skills.

University should also remind them to use strong and unique passwords and encourage them to use multi-factor authentication for institutional accounts. It is important to educate students on the dangers of using a re-used password and predictable passwords. These practices can be reinforced with regular reminders and by institutional security guidelines.

Phishing awareness needs to be strengthened as phishing emails, messages and websites continue to be a significant cybersecurity risk. Periodic phishing awareness exercises could be held at universities and feedback on the awareness provided could be given immediately to the students who participate in such exercises and interact with the simulated suspicious communication.

Digital-Literacy training should also include privacy protection. Students should be advised on privacy settings, sharing of personal information, security in social media and risks of using information that is available to the

public. Moreover, universities should promote students to keep their operating systems and programs up to date, maintain antivirus defenses and lock devices.

Last, larger and more diverse samples of students from various universities should be studied to further understand cybersecurity behavior. Longitudinal studies also could assess if cybersecurity awareness courses lead to long-term changes in digital behaviors among students.

**REFERENCES**


1. Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465
2. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. https://doi.org/10.48550/arXiv.1901.02672
3. Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop* (pp. 47–58). ACM. https://doi.org/10.1145/1595676.1595684
4. Blythe, J. M., Coventry, L., & Little, L. (2011). Unpacking security policy compliance: The motivators and barriers of end user security policy compliance behavior. *Proceedings of the 5th International Conference on Information Security and Assurance*, 13–24.
5. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.
6. Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the 2nd Symposium on Usable Privacy and Security* (pp. 79–90). ACM. https://doi.org/10.1145/1143120.1143123
7. Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873–2882). ACM. https://doi.org/10.1145/2702123.2702243
8. Furnell, S., & Rajendran, A. (2017). The need for a global security awareness program. *Computer Fraud & Security, 2017*(12), 14–17. https://doi.org/10.1016/S1361-3723(17)30074-4
9. 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
10. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6
11. 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
12. McCormac, A., Calic, D., & Parsons, K. (2017). A model of information security culture and its relationship with security outcomes. *Computers & Security, 68*, 1–15.
13. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
14. Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. In *Proceedings of the 12th International Conference on Computer and Information Systems* (pp. 1–6). IEEE.
15. 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. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). ACM. https://doi.org/10.1145/1753326.1753383
16. Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An empirical study. *Information & Management, 51*(2), 145–155. https://doi.org/10.1016/j.im.2013.12.006
17. Stobert, E., & Biddle, R. (2014). The password life cycle: User behaviour in managing passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security* (pp. 243–255). USENIX Association.
18. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems, 24*(6), 659–678. https://doi.org/10.1057/ejis.2015.12

19. Wash, R. (2020). How experts differ from other users in cybersecurity risk perception and cybersecurity advice. *Proceedings of the ACM on Human-Computer Interaction, 4*(CSCW2), 1–27. https://doi.org/10.1145/3415166