Journal of
Information Technology,
Cybersecurity, and Artificial Intelligence

(RESEARCH)

Measuring Cybersecurity Awareness of Students: A Study of State College Students

Dr. Ahmed Al Zaidy

Florida State College at Jacksonville

Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2025, 2(1), 17–40

Article DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Abstract

This study investigates the level of cybersecurity awareness and online security behavior among State College students, utilizing a 54-item structured questionnaire. The survey was administered online via Microsoft Forms over a period of 204 days, yielding 135 responses, of which 128 were retained after data cleaning and processing. The instrument captures four dimensions: demographic characteristics, conceptual knowledge of cybersecurity, self-reported security practices, and behavioral responses to realistic digital scenarios. A descriptive analysis of the responses reveals that students possess a relatively strong conceptual understanding of the selected security principles. For example, more than 95% correctly identified the characteristics of a strong password, and 83.7% reported maintaining an active and regularly updated antivirus program. However, behavioral data reveal inconsistent application of this knowledge in practice. Many students continue to reuse passwords, connect to unsecured Wi-Fi networks, or rely on public devices and unverified software sources when under pressure for convenience or time. An overall awareness score computed from the behavioral items averaged 77.28% on the adopted awareness scale, indicating that a substantial proportion of students exhibit risk-prone habits despite their baseline knowledge of cybersecurity. These findings highlight a persistent knowledge–behavior gap and underscore the need for targeted educational interventions. The study recommends scenario-based awareness training, integration of cybersecurity content across curricula, and institutional policies that reinforce secure digital habits among students.

Keywords— Cybersecurity Awareness (CSA), questionnaire, protection, Awareness behavior

1. Introduction

Cybersecurity refers to the security of information and data that takes into account digital and computing equipment, including computers, servers, smartphones, and the Internet. Cybersecurity is the entirety of computer/network security, protecting equipment against illegal access, modifications, and information system destruction. Given the increasing use of computers and reliance on the Internet, Cybersecurity is a crucial component of any information system.

The elements that increase the possibility of malicious software infecting a system or network are known as Cybersecurity vulnerabilities. When one acknowledges that an attack has compromised a system, it indicates that the framework was compromised and is still operational. Assuming that the system was defenseless against the attack, the term "vulnerability" can be used to describe the quirks of the system that render it defenseless against the attack, the quirks of all frameworks that render them defenseless against an attack of a similar nature, or the quirks of all frameworks that render them defenseless against all attacks [1].

Malware is used regularly throughout internet services to infiltrate devices and launch attacks that leave devices, networks, and data exposed. By 2008, eleven million malware variations had been identified, according to the Osterman research report, and 90% of these malware instances originated from covert downloads from well-known and reputable websites. Network security is a vast and multifaceted topic. However, due to its connections with broader concepts such as "The State," "The Society," "The Nation," and "The Economy," it acquires significant political relevance [2].

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

1.1. Problem Statement

Information Technology (IT) encompasses all technologies, including hardware, software, and communication techniques. IT risks can be categorized into three primary groups: operational risks, security risks, and risks associated with the organization and its personnel. As the use of the Internet has grown, so too have these risks. Security risks, in particular, are linked to vulnerabilities within the core components of IT infrastructures, including software, hardware, and networks. To secure these elements, three critical measures are employed: accountability mechanisms to detect malicious activities, perimeter defense systems to protect against infrastructure breaches, and access control systems to manage data authorization.

College students, as heavy users of digital networks, are expected to be among the most cybersecurity-aware groups. Developing a cybersecurity awareness culture should begin early, and students on the verge of entering the workforce are at a critical stage for building this awareness. The variety and sensitivity of student data make its protection vital, as any alteration, distortion, or compromise could lead to significant issues. IT systems and cyber networks holding student data must be handled with care to ensure confidentiality and security, as they are exposed to numerous threats.

A lack of cybersecurity awareness among students can increase their susceptibility to cyber threats. Therefore, fostering a culture of awareness among students before they transition into the workforce is essential. A key step in this process is assessing and measuring the level of cybersecurity awareness among students at State College. This will help in understanding the gaps and taking proactive steps to secure their data and mitigate associated risks.

1.2. Research Objectives

End users are often regarded as the weakest link in cybersecurity. If students are not sufficiently aware of security threats, they cannot be expected to identify, avoid, report, or mitigate them. As State college students are on the verge of entering the workforce, they must be prepared and knowledgeable about security risks to prevent becoming victims of cybercrime. This study aims to assess the current level of cybersecurity awareness among students at State College. Given the increasing importance of online security in our interconnected global society, cybersecurity awareness must be prioritized within educational systems to ensure safety in digital environments.

1.3. The research questions

In this search, we will focus on the importance of measuring cybersecurity awareness among college students at state institutions by answering the following questions.

Q1: How much do students know about information security?
Q2: What can be done to make sure students remain safe in online communities?

1.4. Research Hypothesis

Based on these research questions, the research hypotheses of this research can be summarized as follows:

H1. All State College students use multiple digital devices daily, whether in social or academic tasks.
H2. Even with new systems being formed every day, systems that are supposed to be impenetrable and largely safe from both external and internal assaults still fall victim to cyberattacks, as system vulnerabilities continue to be exploited.
H3. State College students have sufficient awareness of Cybersecurity risks.

2. Background and RELATED WORKS

Cybersecurity has become an indispensable part of protecting personal and sensitive information, not only for individuals but also within educational environments. As highlighted in recent studies, cyberattacks such as phishing, ransomware, and identity theft pose a significant threat to the integrity of personal data. These risks are especially pronounced among college students, who often underestimate the importance of using strong passwords, regularly updating software, and maintaining secure online behavior. The increasing reliance on digital networks for both academic and personal use underscores the need for proactive cybersecurity education. Institutions must prioritize building cybersecurity awareness to mitigate vulnerabilities that could expose student data to unauthorized access and misuse. In response to these growing concerns, our study examines cybersecurity awareness among State College students, measuring their ability to recognize and respond to potential threats to foster a culture of digital security [27].

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Recently, the rapid development of new technologies has been accompanied by a rise in security compromises. However, there are also many ways in which users can protect themselves while navigating virtual environments. Authors [3] explored the relationship between the increasing rate of global cyber connectivity and the growing vulnerability to hacking activities. They identified five key factors contributing to the rise in risks and the decline in cybersecurity:

The continuous evolution of organizations often creates complexities that negatively impact the strength of their cybersecurity measures.

Mobile computing has blurred the boundaries between organizations and users, as IT moves closer to end-users and further away from the organization, making data more accessible and widespread.

The growing integration of digital systems into daily life has increased the likelihood of cybercrime in both work and home environments.

Cloud-based services and third-party data management and storage solutions introduce new risk channels for sensitive information.

The emergence of closed infrastructure systems in operational technologies, such as power generation and transportation networks, has driven cybercriminals to target these critical, digitalized systems.

There are several common methods used to compromise systems, often referred to as hacking techniques, which include the following [4]:

Malware: This is one of the most prevalent threats in cyberspace, exploiting system vulnerabilities or utilizing new technologies to compromise systems. Malware comes in various forms, such as bots, Trojans, viruses, worms, and rogue software. These malicious programs can enter systems through infected files or websites, granting hackers unauthorized access. Malware targets a wide range of systems, including end-user devices, servers, network infrastructure, and process control systems, such as Supervisory Control and Data Acquisition (SCADA) systems.

Denial-of-Service (DoS): Distributed Denial-of-Service (DDoS) attacks have evolved. In a DDoS attack, numerous compromised computers simultaneously send massive amounts of data packets to a target server, overwhelming it and rendering it unusable. Attackers often exploit the lack of security in average home computers by installing malicious software that enables them to control these machines and launch DDoS attacks remotely.

Internet Protocol (IP) Spoofing: IP spoofing is a technique where the attacker alters the source IP address in data packets, replacing it with a false one. This method disrupts the normal trust relationship between two systems, allowing the attacker to communicate as though they are a legitimate source, potentially leading to further attacks.

Spyware: Spyware is a type of malware that secretly infiltrates computers, often without the user's knowledge. Once installed, spyware can gather information from the victim's system and send it to another location, or even take control of the victim's computer remotely.

Bots: Bots are small programs that perform automated tasks over the Internet. They can be used for benign purposes, but in malicious contexts, they form "botnets" controlled by a central command to carry out tasks such as harvesting email addresses (spam bots), spreading viruses and worms, executing file comparisons, and automating purchases of concert tickets. Botnets can also be used for coordinated attacks on networked systems [5].

Network Intrusion: A network intrusion occurs when an unauthorized individual or system gains access to a company's network or a specific machine within that network. Intrusions can originate from external sources or from internal users, such as employees or clients. Some intrusions are designed to deface websites with offensive messages or images. In contrast, others are more malicious, seeking to steal sensitive information and continue siphoning data until they obtain what they are targeting.

2.1. Related Works

The author in [6] examined student awareness at a higher academic institution, specifically focusing on their engagement with social media platforms. The study revealed that students frequently use popular social media platforms like Facebook, Twitter, LinkedIn, and YouTube. The University of Technology utilized its presence on these

platforms to assess students' cybersecurity awareness. The study found a lack of student engagement with available cybersecurity awareness initiatives. The author suggested that academic institutions could leverage social media to regularly provide cybersecurity awareness materials, thereby enhancing students' knowledge and awareness.

In [7], the authors emphasized the importance of cyber situation awareness for log analysts, enabling them to detect malicious activities, understand threats, and anticipate future consequences. They developed and validated a technique to measure the situation awareness of log analysts, particularly during practical exercises. This validation involved two questionnaires targeting different roles in log analysis, as well as an exercise with five professionals. The findings indicated that the technique could effectively evaluate the analysts' ability to track incidents.

To address similar issues, a framework was proposed in [8] to help network analysts evaluate the security situation of a network and improve their awareness by considering three dimensions: threat, vulnerability, and stability. The framework combines these dimensions to provide a comprehensive understanding of the network's overall security.

In [9], the researchers analyzed information security (IS) awareness in the Middle East, specifically within educational environments that involved undergraduate students, researchers, academic staff, and employees. The study revealed a significant lack of knowledge regarding IS principles, as participants often carried out daily tasks without a thorough understanding of the fundamentals of IS. The researchers highlighted the risks posed by this lack of awareness and recommended implementing training and awareness programs, along with security measures, to enhance data security within academic institutions.

Several studies [10, 11, 12] have focused on raising cybersecurity awareness among university students, while [13] attempted to measure the level of parental awareness regarding cybersecurity to protect their children. Using quantitative data analysis, they measured parental knowledge of cyber threats and protective measures.

Research in [14, 15] identified employees as the most vulnerable link in cybersecurity. These studies emphasized the need for employee cybersecurity awareness and training to defend against evolving threats. The researchers proposed the "Analyse-Predict-Aware-Test" (APAT) model, supported by algebraic equations, to proactively enhance cybersecurity by educating employees about emerging threats and the necessary steps to take when suspicious activity is detected. Other studies [16, 17] introduced models aimed at mitigating security and privacy risks in big data systems caused by employee vulnerabilities.

The authors of [18] investigated the cybersecurity awareness of the general public in Saudi Arabia. The study examined various aspects, including demographics, cybercrime awareness, cybersecurity practices, and incident reporting. Through an online survey, the authors found that while Saudi citizens were knowledgeable about IT, they had limited awareness of cyber threats, practices, and the roles of organizations and government in ensuring online safety. The study recommended developing a model to raise cybersecurity awareness to reduce cybercrime in the region. In a related study [19], conducted in the UAE, Fadi reviewed the need for security education, training, and awareness programs, focusing on phishing risks, wireless security in Dubai and Sharjah, and Radio-Frequency Identification (RFID) security. The study highlighted the need to enhance cybersecurity awareness in schools, universities, and both private and government sectors.

A recent study [20] conducted across four countries—Palestine, Slovenia, Poland, and Turkey—investigated cybersecurity awareness, noting differences in respondents' countries and gender. Numerous studies [21, 22] have proposed models to measure and improve cybersecurity awareness, emphasizing the importance of measurement as a critical step towards building effective information security. A dynamic model [23, 24] has been highlighted as superior due to its structured, leveled approach, which can be applied across different groups and capabilities.

3. RESEARCH METHOD

The present study employed a quantitative research design to measure cybersecurity awareness among students at State College, using a structured 54-item questionnaire. The survey instrument contained four sections: demographic information, conceptual cybersecurity knowledge (yes/no items), cybersecurity-related behaviors (18 Likert-type items scored −1, 0, +1), and multiple-choice scenario questions assessing real-world digital decisions. The questionnaire was distributed online via Microsoft Forms over 204 days, resulting in 135 submissions; after data cleaning, 127 complete responses were retained for analysis.

3.1. Instrument Development

Survey items were derived from established cybersecurity awareness frameworks, including SANS user-awareness guidelines, prior empirical studies in higher education, and best-practice recommendations for password hygiene, phishing identification, removable media handling, and network safety. Domain experts in cybersecurity education reviewed the item pool to ensure conceptual coverage, relevance, and clarity. Items were mapped into three behavioral domains: password practices, online trust/social engineering, and operational digital caution.

3.2. Data Processing and Scoring

Likert-type items were coded so that higher values indicated safer cybersecurity behavior. Composite indices were created for (1) conceptual knowledge, (2) behavioral awareness, and (3) overall awareness. Scenario-based questions were analyzed using frequency distributions to evaluate common risk-taking behaviors.

3.3. Reliability Analysis

Instrument reliability was assessed using Cronbach's Alpha (α), computed for the full behavioral scale and for conceptually derived subscales. Alpha-if-item-deleted diagnostics were examined to ensure no item substantially reduced internal consistency. Reliability analysis was conducted using standard statistical procedures.

3.4. Validity Analysis

Construct validity was evaluated using the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy and Bartlett's test of sphericity, followed by exploratory factor analysis (EFA) using Principal Axis Factoring. Factor extraction was guided by eigenvalues greater than 1, and scree plots were inspected, with Varimax rotation applied to enhance interpretability. The resulting factor structure was examined to determine whether behavioral items clustered into meaningful, theoretically consistent components.

Criterion-related validity was assessed by correlating the composite behavioral awareness score with self-reported online incident outcomes (cyberbullying victimization, impersonation, and cyberbullying perpetration). This allowed for the examination of whether lower awareness predicts higher digital risk experiences.

3.5. Statistical Analyses

Descriptive statistics, reliability coefficients, validity metrics, correlations, and factor loadings were computed using standard statistical tools. Inferential procedures (t-tests, ANOVA, or regression) may be incorporated in subsequent phases, but were not required for the construct validation reported here.

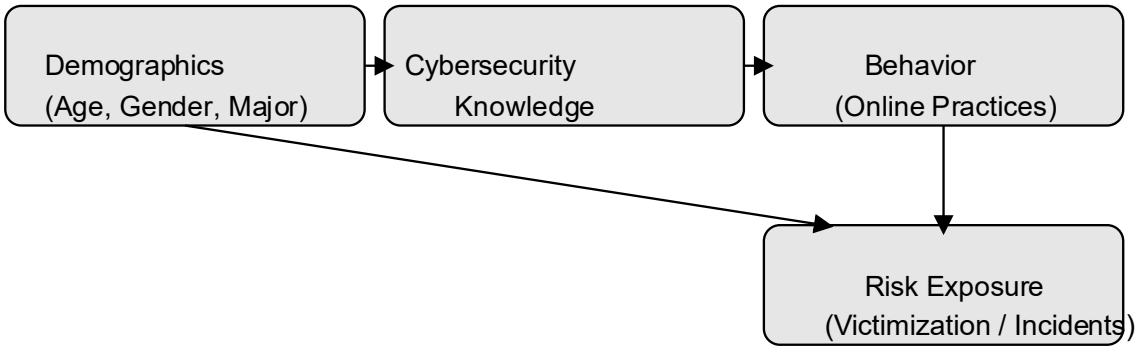
3.6. Conceptual Model of Cybersecurity Awareness

To guide the analytical approach, a conceptual model was developed to represent the hypothesized relationships among the study's core constructs. The model is grounded in behavioral cybersecurity literature, which posits that demographic characteristics influence both cybersecurity knowledge and behavioral decision-making, and that knowledge, in turn, shapes behavioral responses to digital threats. Behavior ultimately predicts individual cybersecurity risk levels, while certain demographic factors may exert direct effects on behavior independent of knowledge.

The model, therefore, includes four linked components: **Demographics → Knowledge → Behavior → Risk**, with an additional direct pathway, **Demographics → Behavior,** to capture potential non-cognitive influences on security practices. This framework supports the study's variable structure, informs validity testing, and provides a theoretical basis for interpreting behavioral outcomes.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Fig. 1 illustrates the conceptual model employed in this study.



4. FINDINGS and DISCUSSION

4.1. RESULTS: RELIABILITY AND VALIDITY

4.1.1. Reliability Results

Cronbach's Alpha for the 18-item behavioral scale was **$\alpha = 0.63$**, indicating acceptable internal consistency for an exploratory awareness instrument. Subscale reliability values were $\alpha =$ **0.38** for password practices and $\alpha =$ **0.59** for social engineering/online trust behavior. No item meaningfully increased the overall Alpha when removed, indicating that all items contributed sufficiently to the measurement construct.

4.1.2. Construct Validity Results

The Kaiser–Meyer–Olkin statistic was **KMO = 0.58**, which meets the minimum threshold for factor analysis. Bartlett's test of sphericity was significant, **$\chi^2(153) = 400.44, p < 0.001$**, indicating that the correlation matrix was suitable for extracting latent dimensions. Exploratory factor analysis identified **three interpretable factors**, reflecting (1) risk-prone social and financial behavior, (2) cognitive security awareness and skepticism, and (3) operational caution in digital interactions. These three components together explained **35.6%** of the total variance.

4.1.3. Criterion-Related Validity

The behavioral awareness composite score demonstrated meaningful relationships with reported online incidents. Most notably, awareness was negatively correlated with cyberbullying perpetration (**$r = -0.23, p < 0.05$**), indicating that students with weaker cybersecurity behaviors are more likely to engage in harmful or unethical online actions. Correlations with cyberbullying victimization and impersonation were negative but non-significant, consistent with the understanding that multiple contextual factors beyond individual behavior influence victimization.

Table 1: Summary of Reliability, Validity, and Factor-Analytic Metrics for the Cybersecurity Awareness Instrument

Metric	Result	Interpretation
Cronbach's Alpha (overall behavioral scale)	0.63	Acceptable reliability for exploratory research
Subscale Alpha – Password Practices	0.38	Low homogeneity; items measure varied behaviors
Subscale Alpha – Social Engineering/Trust	0.59	Moderate reliability
KMO Measure	0.58	Adequate for factor analysis

Bartlett's Test of Sphericity	$\chi^2(153) = 400.44$, $p < 0.001$	Correlation matrix suitable for EFA
Number of Factors Extracted	3 factors	Supports a multidimensional construct
Total Variance Explained	35.6%	Acceptable for human-behavior cybersecurity studies
Criterion Validity (Awareness vs. Cyberbullying Perpetration)	$r = -0.23$ ($p < 0.05$)	Lower awareness predicts higher harmful behavior

4.2. Descriptive Findings

For this research purpose, a survey will be conducted to assess university students' awareness of cybersecurity threats. The data gathered from the students' responses will help determine their level of awareness regarding information security threats. This section presents the statistical results obtained from the questionnaire responses, which aim to achieve the study's objectives. The data was analyzed using Microsoft Excel to compute various statistics. The responses were compiled and recorded to calculate the frequencies and percentages for each question, as illustrated in Table 2. Descriptive statistics were selected as the analytical approach for evaluating the collected data from the questionnaire.

Table 1 Gender of Respondents

Gender	Frequency	Percentage
Male	59	43.7%
Female	67	49.6%
Non-binary	4	3.0%
Prefer not to say	2	1.5%
Total	135	100%

4.2.1. Response Rate

Cybersecurity awareness of students is measured through a Security Awareness Survey. This survey was designed to ask students how they would respond to specific security-related questions and scenarios. The researcher distributed the questionnaire online, requesting participants to complete and submit it promptly. A total of 135 questionnaires were submitted, resulting in a valid response rate of 94.8% (128) of the total sample, as shown in Table 2.

4.2.2. Statistical results

The survey was posted on Microsoft Forms for a period of 204 days, during which students were invited to participate voluntarily. The survey consisted of 54 questions, all of which each student was required to answer. Each question provided a set of values to indicate either strong awareness and good security practices or weak awareness and poor security practices. The questions were divided into three categories:

1. Some questions were structured as true or false to assess students' understanding and awareness of cybersecurity concepts.
2. Another group of questions used a modified Likert scale with risk values of -1, 0, and +1 (Agree, Do not Know, Disagree). Instead of the traditional positive scale, this approach used negative, neutral, or positive values to measure awareness. The results from these questions can be used to calculate the overall sensitivity to risk and the vulnerability score of students, as explained in [25]. These questions were designed to measure online cybersecurity behavior. The risk value of each question was multiplied by the number of times it was chosen by participants to reflect specific cybersecurity behaviors. To determine the awareness of the risk level for each question, the cumulative response was divided by the number of survey participants, yielding an awareness score for each question, as outlined in Table 3.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Table 2: Awareness Score Analysis.

Students' awareness score of risk level	Description
Low (10-25)	Students are aware of Security threats and how to mitigate them. They possess knowledge of security standards and policies and apply them accordingly.
Below Average (25-50)	Students are aware of security threats and know security policies and standards, but they do not apply them effectively.
Average (51-75)	Students are aware of security threats; however, they often lack knowledge of security standards and policies, and consequently, they do not take any measures to protect themselves or participate in activities that put them at risk.
High (76-100)	Students are not aware of security threats and policies. They participate in activities that can be easily exploited.

The data obtained from the cybersecurity awareness survey were exported from Microsoft Forms into an Excel file for analysis and further processing. The dataset contained 135 submitted questionnaires, of which 128 were validated and included in the final analysis after removing incomplete or inconsistent responses. The statistical output was processed using spreadsheet tools and organized into tables and figures for interpretation.

The results include frequency tables, percentage distributions, descriptive statistics, and charts that illustrate students' cybersecurity awareness across different dimensions. Pie charts visualize key variables and their response patterns, while Table 4 provides a detailed numerical representation of student responses to core cybersecurity concept questions. This table summarizes each item, including the frequency and percentage of each response, as well as the researcher's analysis/commentary regarding the students' cybersecurity awareness.

Table 4 Cybersecurity Concepts and Awareness Part.

Cybersecurity Concept / Awareness Question	No %	Yes %	Analysis
Do you have prior knowledge about cybercrimes?	23%	77%	Most students reported having prior knowledge about cybercrimes, suggesting a generally strong foundational awareness. However, nearly one-quarter lack this basic understanding, indicating that introductory cybersecurity education remains necessary.
Do you have sufficient information about cybersecurity and its roles?	25%	75%	Three-quarters of respondents believe they have a good understanding of cybersecurity and its importance. The remaining 25% represents a significant minority who may be unaware of key security responsibilities, suggesting gaps in formal training or exposure.
Do governments supervise the Internet?	8%	92%	Most students believe that governments supervise and regulate the Internet. This high percentage reflects awareness of digital governance but may also indicate misconceptions about the extent of governmental oversight.
In your view, does a strict law reduce cybercrime?	66%	34%	A majority (66%) believe that stricter laws can reduce cybercrime, indicating confidence in the legal deterrent. However, a considerable minority (34%) may believe that cybercrime persists regardless of legal frameworks.
Does focusing on awareness and education reduce cybercrime?	8%	92%	Nearly all respondents recognize the importance of cybersecurity education. This suggests strong support for awareness-based prevention strategies, reinforcing the need for institutional training programs.

Do you have prior knowledge about Information Security?	23%	77%	The distribution mirrors Question 1, indicating that while many students understand basic information security concepts, a substantial 23% remain underinformed and at higher risk.
Is your home computer connected to the Internet?	0%	100%	All respondents have internet-connected devices at home, confirming full exposure to online threats and the necessity of secure online practices.
Is the firewall on your computer enabled?	8%	92%	Most students report having active firewalls, reflecting good basic security hygiene. The 8% without firewall protection or unsure about their status likely represent a vulnerable subset that needs immediate training.
Does anyone have your computer password?	77%	23%	A concerning 77% share their computer password. This indicates extremely weak security behavior and demonstrates a major awareness gap regarding account privacy and unauthorized access risks.
Is antivirus software currently installed on your computer, updated regularly, and enabled?	14%	86%	A large majority maintains up-to-date antivirus software, which is a positive indicator of protective behavior. 14% of the cases without updated antivirus software represent preventable vulnerability cases.
Do you use two-factor authentication when possible?	6%	94%	High adoption of two-factor authentication reflects excellent awareness of modern security practices. The small percentage not using 2FA may lack technical knowledge or access to compatible systems.
Do you update your antivirus regularly?	31%	69%	Although most students perform updates, nearly one-third do not update frequently enough. This group faces significantly higher exposure to malware and outdated threat definitions.
Do you connect your mobile device to public networks?	57%	43%	Over half frequently connect to public Wi-Fi, exposing themselves to risks such as man-in-the-middle attacks. This reflects a serious gap between theoretical understanding and real-world behavior.
Have you been cyberbullied?	84%	16%	While most have not experienced cyberbullying, 16% reporting victimization is significant. This reinforces the importance of digital safety education and reporting mechanisms.
Someone else has pretended to be me online.	76%	24%	Nearly one-quarter experienced impersonation attacks, indicating a substantial prevalence of identity-related threats among students.
Have you pretended to be someone else online?	97%	3%	Only a small proportion of students admit to engaging in impersonation behavior, suggesting that most students do not participate in unethical online practices.
Have you used the same password for everything that needs a password	62%	37%	A majority (62%) reuse the same password across multiple accounts, indicating poor password practices and significantly increased vulnerability to credential-stuffing attacks.
Do you check for viruses when downloading a file or opening an email attachment?	29%	71%	Most students (71%) report scanning or verifying files before opening them, indicating good awareness of malware risks. However, the remaining 29% represent a significant at-risk group, as failing to check downloads and email attachments is a primary cause of malware infections, ransomware attacks, and phishing-related compromises.
Do you use instant messaging programs (for example: Facebook, Instagram, etc.)?	15%	85%	Most students (85%) actively use instant messaging platforms, which reflects high engagement in online social communication. This also increases exposure to security threats such as phishing links, impersonation, malicious attachments, and social engineering. Regular users of messaging apps must therefore be targeted with higher-priority awareness training.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

4.3. Behavioral Cybersecurity Patterns

The following section presents the results of students' online cybersecurity behavior. Table 5 summarizes the awareness scores for each item based on the risk weighting defined in Table 3. For simplicity, all questions were assigned an equal weight, and the overall cybersecurity awareness score was calculated as the average of all awareness-related questions. The overall awareness score of the students is 62.63%. Based on the awareness scale, this places students in the "Average" awareness level, which corresponds to moderate risk behavior and a limited

Table 5: Awareness Score of Cybersecurity Behavior Online.

Questions	The answer that raises awareness		Awareness Score
	Answer	%	
The password does not follow the keyboard pattern	Agree	65.19%	Average
Password consists of lowercase, uppercase, numbers, and special characters	Agree	95.56%	High
Passwords longer than eight characters	Agree	94.81%	High
Passwords based on personal information	Disagree	75.56%	Average
Never change password	Disagree	85.19%	High
Usage of the "Remember my password" option	Disagree	34.07%	Below Average
Used to write down the password	Disagree	59.26%	Average
Never use "hint" to recover a forgotten password	Agree	39.26%	Below Average
Established a trusted online relationship with strangers	Disagree	79.26%	High
Ignored emails from well-known organizations about unusual or too-good-to-be-true announcements	Agree	82.22%	High
Respond to SMS announcing contests with huge sums of money	Disagree	94.81%	High
Never trust strangers' information given on the Internet	Agree	90.37%	High
Never consider any amount of money for services offered by an online site	Agree	77.04%	High
Willing to deposit the money requested by online friends	Disagree	90.37%	High
Aware of and able to identify the latest online scams	Agree	78.52%	High
Trust strangers' pictures posted on the Internet	Disagree	85.93%	High
Never receive parcels and gifts from Internet friends	Agree	75.56%	Average
Would not hesitate to meet Internet friends face-to-face	Disagree	60.00%	Average
Mean		77.28%	High

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

4.4. Scenario-Based Judgment Results

The next section will present the results of the questions of the closed-list answer, as follows:

The results presented in Figure 2 show clear variation in students' cybersecurity response behavior when encountering an unexpected file. A majority of participants (65%) exhibit secure behavior by deleting the file immediately without opening it, demonstrating strong awareness of potential malware, phishing attachments, or social engineering threats.

An additional 24% adopt another safe practice—meaning they scan files for viruses before opening them—which indicates a proactive approach to risk mitigation. Together, these two groups represent 89.2% of respondents demonstrating appropriate cybersecurity behavior in this scenario. However, a smaller proportion of students display high-risk behavior. Notably, 5 % reported opening the file to see what it contains, which exposes them to malware, ransomware, or remote-execution attacks. The 6 % answering "None of the above" may also represent students who are unsure of the correct action, highlighting another gap in security awareness.

Overall, these findings suggest that while most students understand the risks associated with unexpected files, a minority continue to engage in behaviors that expose them to significant cyber threats. Targeted awareness training remains essential for reinforcing safe practices.

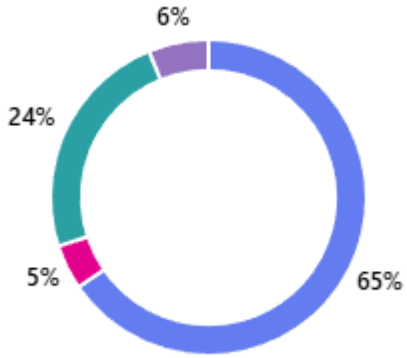


Fig. 2: When you receive a file that you are not expecting, you typically

Figure 3 illustrates students' self-reported ability to respond to a cybersecurity incident involving a hacked computer. The majority of respondents (74%) indicated that they are aware of the steps to take if their computer becomes compromised. This suggests that most students possess at least a foundational understanding of incident response actions such as disconnecting from the network, running antivirus scans, changing passwords, or seeking IT support.

However, a significant minority (26%) reported that they would not know how to respond. This is a substantial vulnerability, as students who are unsure how to react to a cyber intrusion are more likely to experience prolonged exposure, data loss, or further exploitation. These results suggest a need for enhanced training on incident response procedures, particularly for non-technical students who may lack prior experience in managing cybersecurity events.

Overall, the findings demonstrate that while a majority of students feel confident in responding to a compromised device, a notable portion remain unprepared, highlighting the importance of integrating basic incident response education into cybersecurity awareness initiatives.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

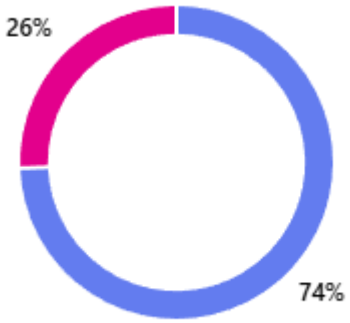


Fig. 3: If Your Computer Got Hacked

Figure 4 shows the types of files students typically download from the Internet. Most respondents (46%) reported downloading applications, which suggests frequent engagement with executable files that may introduce security risks if obtained from untrusted sources. A significant proportion (34%) also downloads documents, which are another common vector for malware, phishing attachments, and embedded macros.

A smaller portion (13%) downloads other types of files, which may include compressed archives and system utilities. Finally, 6% reported downloading movies or songs, a behavior often associated with unregulated or piracy websites known to host malicious content.

The variation in download behavior highlights the importance of teaching students how to verify file authenticity, check digital signatures, and avoid software repositories or file-sharing sites that lack proper security controls. Although downloading content is a common online activity, it remains a high-risk area where unsafe practices can easily lead to system compromise.

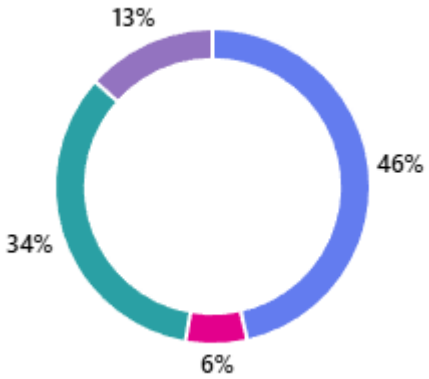


Fig. 4: Do you download from the Internet?

Figure 5 illustrates the frequency with which students update their antivirus software, a key indicator of proactive device security management. The majority of respondents (75%) reported that their antivirus updates are automatic, reflecting strong adoption of recommended cybersecurity practices. Automatic updating significantly reduces exposure to new malware variants by ensuring that threat definitions remain current.

Approximately 11% of students update their antivirus software once a month, which is less secure given the rapid evolution of cyber threats. A notable 10% reported that they never update their antivirus software, placing them at high risk of infection by known malware. Additionally, only 5% perform updates once a week, representing a small group that actively maintains their device security manually.

Overall, these results suggest that while most students benefit from automated protection mechanisms, a meaningful minority lack consistent antivirus updating behavior. Cybersecurity training should therefore emphasize the importance of keeping security tools up to date, especially for users who rely on manual update processes.

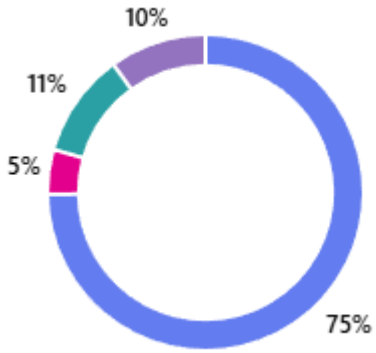


Fig. 5: How regularly do you update your antivirus?

Figure 6 illustrates the types of information students typically share on social media platforms. A substantial majority of respondents (74%) reported that they "know very well what to share" online. This indicates a high level of self-reported awareness regarding appropriate and safe content-sharing practices, suggesting that most students consciously limit their personal exposure on social media.

Approximately 11% of students share only life event updates, which is a moderately safe practice as long as the content does not reveal sensitive personal details. Similarly, 10.4% share pictures only, a behavior that may still pose privacy risks depending on metadata, location information, or the nature of the images.

A small minority (2%) reported sharing everything on social media. This group represents the highest risk category, as oversharing can expose individuals to identity theft, social engineering attacks, stalking, and targeted phishing.

Overall, these results indicate that while most students demonstrate careful and selective sharing habits, a portion still engage in risky online behavior that could compromise their privacy and cybersecurity. This highlights the importance of continuous education on digital footprint management and safe social media practices.

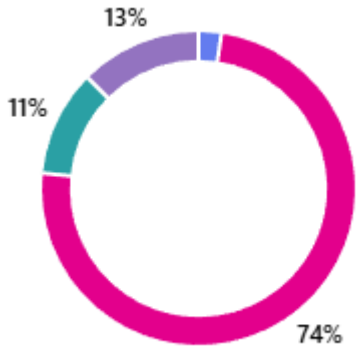


Fig. 6: What kind of information do you share on social media?

Figure 7 illustrates students' password behavior when creating new online accounts. A substantial majority of respondents (76%) reported that they create a strong password and store it in a password management program. This indicates a high level of cybersecurity awareness and reflects adherence to best practices for account security. The use of password managers is considered one of the most effective measures to protect against unauthorized access and credential reuse attacks.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

However, 24% of respondents reported using the same password across multiple websites to make it easier to remember. This behavior is widely recognized as a significant cybersecurity risk, as password reuse greatly increases vulnerability to credential stuffing, phishing, and account takeover attacks. If a reused password is compromised on one platform, all other accounts using the same password become immediately vulnerable.

These findings highlight a notable divide between secure and insecure password habits among students. Although the majority demonstrate strong password management practices, nearly one-quarter rely on risky behaviors that could compromise their online safety. Cybersecurity awareness programs should emphasize the dangers of password reuse and promote the adoption of secure password management tools to enhance online security.

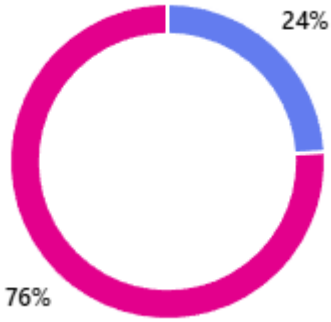


Fig. 7: When you open an account for a website

Figure 8 displays how students respond when they receive email messages containing links to external websites, a scenario commonly associated with phishing attempts. The majority of students (59.0%) reported conducting an online search to verify the legitimacy of a website or link before clicking, indicating a strong awareness of phishing risks and an effort to validate suspicious content.

Another 41% of respondents rely on hovering their mouse over the link to preview the URL before deciding whether to click. This is also a recommended security practice, as it enables users to inspect the destination address without visiting it, helping them identify spoofed or malicious URLs.

Together, these findings demonstrate that students generally adopt cautious behaviors when interacting with unsolicited email links. However, the fact that responses are split between two verification methods may suggest varying levels of technical understanding. Institutions may benefit from reinforcing standardized email safety procedures, such as verifying sender identity, checking for URL mismatches, and reporting suspicious emails, to ensure consistent and robust protection against phishing threats.

Fig. 8: When you receive an email containing links to external websites

Figure 9 illustrates how students approach secure financial browsing when accessing banking or credit-card purchase websites. Most respondents (57%) reported using protected anti-malware browsers, indicating strong awareness of

the sensitivity of online financial transactions. This demonstrates that more than half of the students recognize the need to safeguard their sessions from potential malware, phishing attacks, keyloggers, and unsafe network environments.

Approximately one-quarter (27%) use a regular browser, which exposes them to greater risk, especially if the device is compromised or lacks security updates. This group may be unaware of the additional protection mechanisms offered by secure browsing environments.

A smaller portion (17%) choose incognito/private mode, which provides limited privacy—mainly hiding browsing history locally—but does not protect against phishing, malware, or compromised HTTPS certificates. This suggests a misunderstanding of incognito mode, where students believe it offers security rather than simply reducing local traceability.

Overall, these findings show that while most students adopt appropriate measures when accessing financial websites, a substantial minority still rely on standard or misleading privacy options, leaving their sensitive financial data vulnerable to cyber threats. Continued awareness campaigns should emphasize the difference between privacy tools and genuine security controls and reinforce best practices for financial browsing.

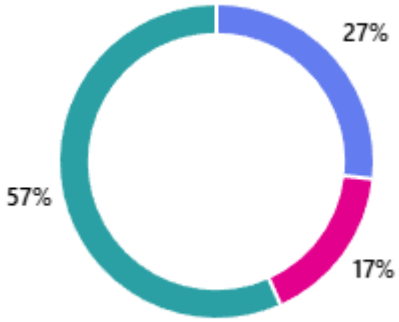


Fig. 9: When you browse a bank or credit card purchase site

Figure 10 illustrates how students respond when encountering a trial version of a program available on an unfamiliar website. Almost half of the respondents (52%) stated that they would not download or install the program, indicating a strong awareness of the risks. This group recognizes that unknown software sources can pose significant threats, including malware, spyware, keyloggers, and ransomware.

A substantial percentage of students (44%) indicated that they would search for program information before downloading it, reflecting moderate awareness of the process. Although this suggests responsible decision-making, it still carries risk, as online reviews and forum discussions can be manipulated and may not reliably guarantee program legitimacy. These students act cautiously but still maintain the possibility of downloading the software if it appears trustworthy.

Only a small portion (4%) admitted they would download the program and try it immediately. This behavior represents the highest-risk group, as downloading from untrusted sources is one of the most exploited cyber-attack vectors. Attackers commonly disguise malicious executables as "free trials," "portable versions," or cracked software to infect systems and harvest personal information.

Overall, the results suggest that most students demonstrate prudent behavior and understand the risks associated with unofficial software sources. However, the presence of even a small group willing to download unknown programs underscores the ongoing need for cyber hygiene education, particularly regarding software authenticity, digital signatures, and the risks associated with pirated or unofficial downloads.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

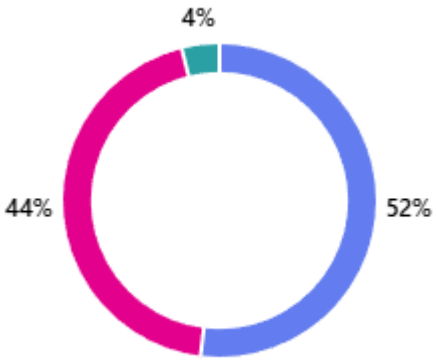


Fig. 10: When you hear about a program and want to try it, I have searched the Internet and found a trial version of the program on an unknown website.

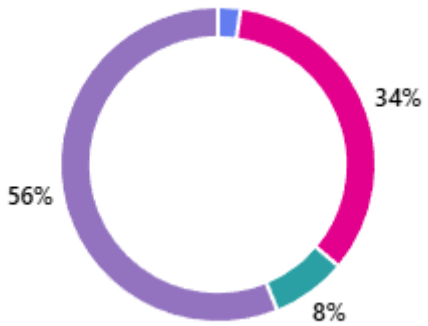
Figure 11 illustrates how students react when encountering an unfamiliar USB flash drive in a public setting. The majority of respondents (56%) selected "None of the above", which generally indicates avoidance or leaving the device untouched. This is a positive cybersecurity behavior, as it reduces the likelihood of exposing a workstation to malware delivered through USB autorun functions or hidden payloads.

A considerable portion (34%) reported that they would take the USB to the receptionist or a responsible authority to attempt to find the owner. While this behavior demonstrates good ethical intentions, it may still pose a risk if the USB is plugged into an unprotected workstation. Institutions should establish secure collection procedures or official lost-and-found protocols to handle unknown devices safely.

A smaller group (8%) indicated that they would open the USB drive using a sandbox, which reflects a higher level of technical awareness. Although sandboxing offers isolation, it is not foolproof and may fail to contain firmware-level threats, USB Rubber Ducky payloads, or BadUSB exploits.

The riskiest behavior—opening the USB to see what is inside—was selected by 2% of respondents. This group is highly vulnerable to cyberattacks because malicious USB devices can execute code immediately upon connection, without user interaction.

Overall, the results in Fig. 11 suggest that while most students avoid interacting with unknown USB devices, a notable minority still engage in risky behaviors. This highlights the importance of digital forensics awareness and proper handling of unknown removable media, especially in cybersecurity training programs.



DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Fig. 11: You found a USB flash drive while going to work

Figure 12 examines students' reactions when they urgently need internet access and encounter a free, unsecured Wi-Fi hotspot without a password. The largest group of respondents (48%) chose not to connect ("None of the above"), indicating strong awareness of the security risks associated with open wireless networks. This behavior greatly reduces exposure to man-in-the-middle attacks, packet sniffing, and credential theft.

A substantial proportion (38%) stated they would connect and use a VPN. This reflects a relatively high level of technical awareness: students in this group recognize the risks of open Wi-Fi and attempt to mitigate them by encrypting their traffic. While VPN usage significantly improves security, it does not fully eliminate threats such as malicious access points or DNS manipulation; however, it remains a safer option than connecting without protection.

However, 12% of students reported they would connect and browse the Internet without any additional protection, and 3.0% would connect in incognito/private mode. Both behaviors are risky: incognito mode only hides browsing history locally and does not protect against network-level attacks. These students are therefore vulnerable to eavesdropping, session hijacking, and credential compromise.

Overall, the results in Fig. 12 suggest that while a majority of students either avoid insecure Wi-Fi or take steps to secure their connection, a notable minority still undervalues the dangers of open networks. This underscores the need for continued cybersecurity education that focuses on wireless security, rogue access points, and the limitations of "privacy" modes compared to true security measures.

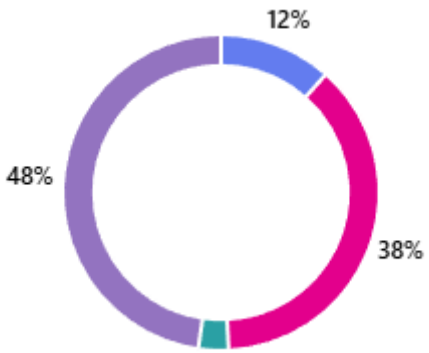


Fig. 12: You were in desperate need of Internet and found a free Wi-Fi hotspot without a password

Figure 13 presents students' behavior regarding the use and maintenance of antivirus programs. A large majority of respondents (83.7%) indicated that their antivirus software is installed, enabled, and updated regularly. This behavior reflects a strong understanding of the importance of ongoing device protection, indicating that most students rely on antivirus solutions to detect and remove potential threats.

Only 13.3% reported not maintaining an updated antivirus program. This group represents a considerably vulnerable population, as outdated or inactive antivirus software fails to protect against modern threats—particularly new malware variants, zero-day vulnerabilities, and phishing-related payloads. These systems are more susceptible to ransomware, spyware, and credential theft.

The results suggest that students generally recognize antivirus software as a critical component of device security. However, the small minority that neglects updating antivirus software could easily become targets for cyberattacks, especially in environments with frequent downloads, external storage usage, or unsecured Wi-Fi connections.

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

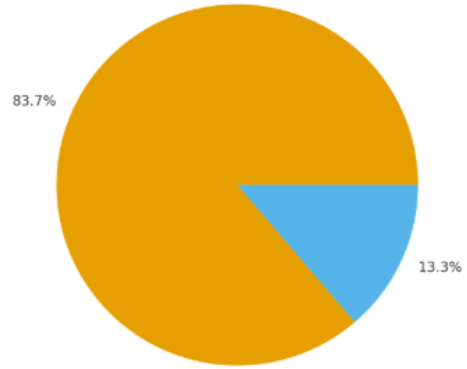


Fig. 13: an antivirus program and remove it from your computer.

Figure 14 illustrates students' password maintenance practices. The overwhelming majority of respondents (85.2%) disagree with the statement "Never change password", indicating that they do regularly update their login credentials. This reflects a strong security posture, as periodic password changes reduce the likelihood of long-term credential compromise, brute-force attacks, or account reuse exploits.

Only 8.9% of students admitted to never changing their password, a risky behavior that increases their vulnerability to persistent cyber threats. Static passwords, especially when reused across multiple accounts, are highly susceptible to credential stuffing, database leaks, phishing, and social engineering attacks.

An additional 3.0% reported uncertainty or lack of awareness regarding their own password update practices. This group may rely on automatic logins or saved passwords without consciously monitoring their security, which can still pose a threat if their accounts become compromised.

Overall, the results demonstrate that most students understand the importance of password rotation. However, a small but significant minority either do not update their passwords or are unsure of their behavior, suggesting the need for continued awareness about authentication hygiene and account lifecycle management.

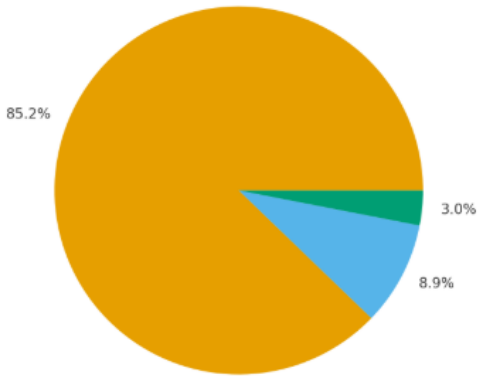


Fig. 14: How regularly should you change the computer/ mail password?

TABLE 5 LISTS THE HIGHER PERCENTAGE ANSWERS OF OPEN QUESTIONS

DOI: https://doi.org/10.70715/jitcai.2025.v2.i3.030

Answer (Highest Selected)	Related Question	Percentage Result
Updated my passwords	*How do you protect yourself online?*	68.1%
Only visit websites if I know and trust them	*What do you do to stay safe when browsing the Internet?*	72.6%
Friends, social worker/support worker	*If you get into online trouble, who do you ask for help?*	47.4%
Websites or apps	*Where do you get cybersecurity information?*	51.9%
Browsing websites and chatting with friends	*What do you do most often when you are online?*	54.8%

TABLE 6 – Highest Percentage Answers of Closed-Ended Cybersecurity Behavior Questions

Related Question	The answer that tends to raise awareness %	Awareness Score Level
When you receive a file that you are not expecting, you typically	65.4%	High Awareness
Do you download from the Internet?	43.7%	Average Awareness
How regularly do you update your antivirus?	72.6%	Average Awareness
What kind of information do you share on social media?	70.4%	Average Awareness
When you open an account for a website	72.6%	Average Awareness
When you receive an email containing links to external websites	57.0%	Average Awareness
When browsing a bank or credit card purchase site	53.3%	Average Awareness
You heard about a program and found a trial version on an unknown website	52%	Average Awareness
You found a USB flash drive while going to work	54.1%	Average Awareness
You were in desperate need of Internet and found free Wi-Fi without a password	45.9%	Below Average Awareness
Use an antivirus program and remove it from your computer	83.7%	High Awareness
How regularly do you change the computer/mail password	85.2%	High Awareness

4.5. DISCUSSION

The overall findings of this study reveal a complex relationship between students' cybersecurity knowledge, their behavioral practices, and their real-world digital decision-making. Although reliability analysis indicated **moderate internal consistency** for the behavioral scale ($\alpha = 0.63$) and construct validity was supported through a three-factor structure, the results underscore a persistent disconnect between conceptual understanding and practical application—consistent with behavioral cybersecurity research in higher education.

The **factor analysis** demonstrated that student behavior in digital environments can be grouped into three latent dimensions:

[1]. *risk-prone social and financial behavior*,
[2]. *cognitive security awareness and skepticism*
[3]. *operational caution in digital interactions*.

This multidimensionality aligns with human-factor models in cybersecurity, such as Protection Motivation Theory and the NIST NICE behavioral competencies, which recognize that knowledge alone does not translate into safe action. Students may understand recommended practices yet still behave in ways that expose them to risk, particularly when convenience or social pressure is involved.

The descriptive findings reinforce this gap. Students demonstrated **strong conceptual knowledge**—with more than 75% reporting prior understanding of cybercrimes, information security roles, and the importance of antivirus protection and multi-factor authentication. However, **behavioral data revealed inconsistencies**. For example, although most students can identify strong password characteristics, **62% reuse the same password across multiple platforms**, a risky habit frequently cited in cybersecurity studies as a primary cause of account compromise.

Similarly, while students showed prudent behavior in some high-risk scenarios—such as deleting unexpected files or avoiding unfamiliar software downloads—their decision-making weakened significantly in contexts involving **public Wi-Fi**, **financial browsing**, and **social trust interactions**. Nearly half use unsecured Wi-Fi networks, often relying on misconceptions such as believing incognito mode provides security. These findings align with prior literature, which indicates that college students often misjudge the severity of network-level threats and overestimate the protection provided by consumer tools.

Notably, the **criterion-related validity** analysis revealed a small but significant negative correlation (**$r = -0.23$, $p < 0.05$**) between behavioral awareness and the perpetration of cyberbullying. Students with lower cybersecurity awareness were more likely to engage in risky or unethical online actions. This reinforces the behavioral–ethical dimension of cybersecurity, suggesting that awareness programs should extend beyond technical safety to include responsible digital citizenship.

The results of this study also highlight disparities across different types of cyber behavior. Students were more confident and consistent in behaviors involving **personal devices** (e.g., antivirus updates, password changes) but far less consistent in behaviors involving **network environments**, **social interactions**, or **external content sources**. This pattern aligns with studies showing that younger digital users often exhibit *device-centric* awareness but lack *ecosystem-level* threat comprehension, particularly in recognizing the risks of public networks or deceptive digital content.

When interpreted in conjunction with the conceptual model, the findings suggest that demographics, baseline knowledge, and scenario-based judgments all contribute to students' overall cybersecurity posture. However, knowledge alone cannot account for variation in behavior. Instead, the factor structure indicates that **social dynamics**, **perceived trust**, **habitual shortcuts**, and **situational decision-making** play critical roles in shaping cybersecurity practices.

Finally, the descriptive behavioral awareness score (77.28%) indicated that the sampled students fall into a category defined as "High" risk behavior, reflecting poor alignment with safe practices. This metric complements the factor-analytic results, underscoring that while students possess foundational knowledge, their behaviors are not consistently protective of it. These findings are consistent with international studies from ENISA and EDUCAUSE, which also observe behavioral vulnerabilities among students who consider themselves knowledgeable about cybersecurity.

Overall, the Discussion indicates that improving cybersecurity outcomes among State College students will require more than information dissemination. Effective interventions must incorporate **applied, scenario-driven training**, emphasize **network and situational risks**, and challenge incorrect assumptions students hold about online safety.

5. CONCLUSION

This study examined cybersecurity awareness among State College students using a structured, multidimensional instrument, whose reliability and construct validity were empirically confirmed. Although students demonstrated moderate internal consistency in their behavioral responses and a valid three-factor awareness structure, the findings

revealed a persistent disconnect between conceptual knowledge of cybersecurity principles and the consistent application of secure behaviors in real-world digital contexts.

Students demonstrated a strong understanding of basic security concepts, including password complexity, antivirus usage, phishing cues, and the importance of education; however, they often engaged in behaviors that contradicted best practices. High-risk behaviors were particularly evident in scenarios involving convenience or social interaction, such as connecting to unsecured Wi-Fi networks, downloading unfamiliar software, and forming trust relationships with strangers online. These results reflect the well-documented "knowledge–behavior gap" identified in cybersecurity literature, where individuals possess technical awareness but fail to translate it into protective habits (ENISA, 2023; SANS, 2022).

The overall behavioral awareness score of 77.28% reflects a level of elevated risk rather than competence, emphasizing that students' self-perceived knowledge does not reliably predict safe cybersecurity behavior. This conclusion is supported by criterion-related validity analysis, which showed a negative correlation between behavioral awareness and engagement in harmful online acts such as cyberbullying. The presence of this behavioral–ethical relationship underscores the importance of viewing cybersecurity competence not merely as a technical skillset, but as a component of responsible online citizenship.

Collectively, the study confirms that effective cybersecurity education for college students must extend beyond conceptual instruction to include practical applications. Students require hands-on, scenario-based experiential learning that challenges their assumptions, strengthens decision-making abilities, and aligns their behaviors with the protective strategies taught in formal awareness programs. As cyber threats continue to evolve and increasingly exploit human vulnerabilities, efforts to reinforce behavioral cybersecurity competence among young adults remain essential to building a resilient digital campus ecosystem.

6. RECOMMENDATIONS AND IMPLICATIONS

The findings of this study indicate that, although students possess baseline cybersecurity knowledge, their behavioral responses remain inconsistent across real-world scenarios. Based on observed gaps and supported by contemporary research, several pedagogical and institutional recommendations are proposed.

6.1. Integrating Scenario-Based and Experiential Learning

Extensive research in cybersecurity education demonstrates that passive instructional formats—such as static awareness campaigns, lectures, and email reminders—rarely lead to long-term behavioral change. The NIST NICE Framework emphasizes that competency develops when learners practice decision-making in realistic, consequence-based environments [40]. Scenario-driven training, including phishing simulations, guided incident response exercises, and safe failure-driven labs, enables students to experience the outcomes of insecure behaviors and reflect on alternative actions. Institutions should therefore embed experiential security modules within general education curricula to strengthen behavioral awareness.

6.2. Implementing Continuous and Adaptive Awareness Programs

Awareness decays over time unless reinforced through ongoing engagement. ENISA's 2023 Awareness and Education Report emphasizes the importance of continuous, adaptive cybersecurity training cycles rather than one-time interventions [27]. Micro-learning modules, delivered quarterly, target scenario challenges addressing Wi-Fi risks, downloads, and authentication, and provide personalized learning pathways for high-risk groups (e.g., first-year students, frequent social media users), helping to maintain elevated awareness levels. Adaptive systems that modify content difficulty based on performance have been shown to enhance retention and long-term behavioral improvement [41], [42].

6.3. Reinforcing Network-Level Security Competencies

Students demonstrated the greatest weaknesses in network-layer judgment, consistent with findings in both academic and industry research. Studies on public Wi-Fi risks show that young adults significantly underestimate man-in-the-middle threats, rogue access points, and packet interception [34], [35]. Training should therefore include demonstrations of Wi-Fi–based attacks, clarification of VPN capabilities and limitations, recognition of rogue networks, and correction of misconceptions such as the false belief that incognito mode enhances security. Such instruction has been shown to improve behavioral outcomes in insecure network environments substantially [29].

6.4. Promoting a Robust Authentication and Password Ecosystem

Although respondents understood the technical components of creating strong passwords, their behavioral follow-through was inconsistent, particularly in terms of password reuse. Modern authentication guidance, including NIST SP 800-63B [31] and Microsoft identity recommendations [32], emphasizes the importance of promoting password managers, minimizing unnecessary password changes, and encouraging the widespread adoption of MFA/2FA. Universities should consider campus-wide password manager licensing, MFA-first login systems, and workshops that translate theoretical password knowledge into sustainable security habits. Research confirms that students are more compliant when institutions provide supported, streamlined authentication ecosystems [20].

6.5. Strengthening Digital Citizenship, Ethics, and Social Responsibility

The correlation observed between lower cybersecurity awareness and increased engagement in harmful online behavior aligns with UNESCO's Digital Citizenship Education Framework [38]. Cybersecurity skills cannot be developed in isolation from broader digital ethics. Universities should incorporate modules on respectful digital communication, identity protection, consequences of online actions, and social engineering awareness. Findings from cyberbullying research further support the integration of ethical and behavioral dimensions into cybersecurity education, enhancing overall digital well-being [39].

6.6. Enhancing Institutional Policy and Governance

Institutional cybersecurity maturity strongly influences user compliance and behavior. Research shows that campuses with structured cybersecurity governance—mandatory onboarding training, periodic assessments, and recurring phishing simulations—report significantly higher levels of student awareness [28], [33]. Universities should adopt secure default configurations across campus systems, develop peer-led cybersecurity ambassador programs, and maintain transparent performance dashboards that track improvement over time. Institutional reinforcement is a key factor in sustaining cybersecurity behavior.

6.7. Directions for Future Research

Future research should expand the scope of this study by conducting multi-campus comparisons to enhance external validity, implementing longitudinal designs to evaluate behavioral change over time, and testing the effectiveness of specific training interventions through experimental or quasi-experimental methods. Emerging machine learning approaches can also be applied to predict at-risk behavioral profiles and tailor awareness interventions more precisely [37], [44]. These directions offer a pathway toward more predictive and personalized cybersecurity education frameworks.

7. References

[1] N. M. Campara, *System Assurance: Beyond Detecting Vulnerabilities*. Burlington, MA, USA: Morgan Kaufmann, 2010. URL: https://www.elsevier.com/books/system-assurance/campara/978-0-12-373583-6

[2] P. W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, U.K.: Oxford Univ. Press, 2013. URL: https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918096

[3] P. V. Kessel and K. Allan, "Get ahead of cybercrime," *EY Global Information Security Survey*, 2014. URL: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2014.pdf

[4] D. Willson, *Cybersecurity Awareness for CEOs and Management*. Elsevier, 2016. URL: https://www.elsevier.com/books/cybersecurity-awareness/willson/978-0-12-802469-0

[5] M. Rouse, "Bot (software robot)," *Techopedia*, 2021. URL: https://www.techopedia.com/definition/10459/bot-software-robot

[6] P. Potgieter, "The awareness behaviour of students on cybersecurity awareness by using social media platforms," *Kalpa Publications in Computing*, vol. 12, pp. 272–280, 2019. URL: https://easychair.org/publications/paper/2G9C

[7] P. Lif, M. Granåsen, and T. Sommestad, "Development and validation of technique to measure cyber situation awareness," in *Proc. CyberSA*, 2017. DOI: https://doi.org/10.1109/CyberSA.2017.8068647 URL: https://ieeexplore.ieee.org/document/8068647

[8] R. Xi, Y. Xiaochun, and H. Zhiyu, "Framework for risk assessment in cyber situational awareness," *IET Information Security*, vol. 13, no. 2, pp. 119–128, 2019. DOI: https://doi.org/10.1049/iet-ifs.2018.5189 URL: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ifs.2018.5189

[9] S. Al-Janabi and I. AlShourbaji, "A study of cybersecurity awareness in educational environment in the Middle East," *J. Inf. Knowl. Manag.*, vol. 15, no. 1, 2016. DOI: https://doi.org/10.1142/S0219649216500076 URL: https://www.worldscientific.com/doi/abs/10.1142/S0219649216500076

[10] E. B. Kim, "Cybersecurity awareness status of business college undergraduate students," *Information Security Journal*, vol. 22, no. 4, pp. 171–179, 2013. DOI: https://doi.org/10.1080/19393555.2013.828803 URL: https://www.tandfonline.com/doi/abs/10.1080/19393555.2013.828803

[11] Y. K. Peker et al., "Raising cybersecurity awareness among college students," *CISSE Journal*, 2016. URL: https://cisse.info/journal/index.php/cisse/article/view/66

[12] K. Senthilkumar and S. Easwaramoorthy, "A survey on cybersecurity awareness among college students in Tamil Nadu," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 263, no. 4, 2017. DOI: https://doi.org/10.1088/1757-899X/263/4/042043 URL: https://iopscience.iop.org/article/10.1088/1757-899X/263/4/042043

[13] N. Ahmad et al., "Cybersecurity situational awareness among parents," in *Proc. Cyber Resilience Conf.*, 2018. DOI: https://doi.org/10.1109/CR.2018.8626830 URL: https://ieeexplore.ieee.org/document/8626830

[14] A. H. Khan et al., "SartCybersecurity Awareness Measurement Model (APAT)," in *Proc. PARC*, 2020. DOI: https://doi.org/10.1109/PARC49193.2020.236622 URL: https://ieeexplore.ieee.org/document/9087075

[15] G. Kemper, "Improving employees' cybersecurity awareness," *Computers & Security*, vol. 2019, no. 8, pp. 11–14. DOI: https://doi.org/10.1016/S1361-3723(19)30085-5 URL: https://www.sciencedirect.com/science/article/pii/S1361372319300855

[16] T. Gundu, "Big data, big security and privacy risks: Bridging employee knowledge and actions gap," Int. J. Cyber Warfare Terrorism, vol. 9, no. 1, pp. 1–16, 2019. DOI: https://doi.org/10.4018/IJCWT.2019010101 URL: https://www.igi-global.com/article/big-data-big-security-and-privacy-risks/231549

[17] L. Hadlington, Employees' attitudes towards cybersecurity and risky online behaviours: An empirical assessment in the United Kingdom" Int. J. Cyber Criminol., vol. 12, no. 1, pp. 1–20, 2018. URL: http://www.cybercrimejournal.com/hadlingtonijcc2018vol12issue1.pdf

[18] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki,"A survey of cybersecurity awareness in Saudi Arabia" in *Proc. ICITST*, 2016. DOI: https://doi.org/10.1109/ICITST.2016.7856687 URL: https://ieeexplore.ieee.org/document/7856687

[19] F. A. Aloul,"Cybersecurity awareness in UAE: A survey paper" in *Proc. Int. Conf. Internet Technology and Secured Transactions*, 2010. URL: https://ieeexplore.ieee.org/document/5599842

[20] M. Zwilling, G. Klein, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim,"Cybersecurity awareness, knowledge and behavior: A comparative study" *J. Comput. Inf. Syst.*, vol. 60, no. 1, pp. 1–10, 2020. DOI: https://doi.org/10.1080/08874417.2020.1712269 URL: https://www.tandfonline.com/doi/full/10.1080/08874417.2020.1712269

[21] M. Evangelopoulou and C. W. Johnson,"Empirical framework for situation awareness measurement techniques in network defense" in *Proc. CyberSA*, 2015. DOI: https://doi.org/10.1109/CyberSA.2015.7166132 URL: https://ieeexplore.ieee.org/document/7166132

[22] S. E. Erol and S. Sagiroglu,"Awareness qualification level measurement model" in *Proc. IBIGDELFT*, 2018. URL: https://ieeexplore.ieee.org/document/8627342

[23] S. S. Tirumala, M. R. Valluri, and G. A. Babu,"A survey on cybersecurity awareness concerns, practices and conceptual measures" in *Proc. ICCCI*, 2019. DOI: https://doi.org/10.1109/ICCCI.2019.8821951 URL: https://ieeexplore.ieee.org/document/8821951

[24] S. T. Human,"Security awareness survey" SANS Institute, 2012. URL: https://www.sans.org/sites/default/files/2018-01/security-awareness-survey.pdf

[25] W. Aljohani et al.,"Cybersecurity awareness among university students" *Int. J. Comput. Sci. Mobile Comput.*, vol. 9, no. 6, pp. 141–155, Jun. 2020. URL: https://www.ijcsmc.com/docs/papers/June2020/V9I6202014.pdf

[26] A. Al Zaidy,"Cybersecurity and personal privacy: Protecting yourself in the digital age" *Open Access Research Journal of Science and Technology*, vol. 12, no. 1, pp. 131–135, Oct. 2024. DOI: https://doi.org/10.53022/oarjst.2024.12.1.0122
URL: https://oarjst.com/index.php/oarjst/article/view/122

[27] ENISA, *Cybersecurity Awareness and Education Report*, 2023. URL: https://www.enisa.europa.eu/publications/cybersecurity-awareness-and-education

[28] SANS Institute, *Security Awareness Report: Managing Human Risk*, 2022. URL: https://www.sans.org/u/1x13

[29] J. Blythe and L. Coventry,"Cyber security behaviours in university students" *Journal of Cybersecurity*, vol. 6, no. 1, 2020. DOI: https://doi.org/10.1093/cybsec/tyaa003 URL: https://academic.oup.com/cybersecurity/article/6/1/tyaa003/5838120

[30] Yeo, L. H., & Banfield, J. (2022). Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. Perspectives in health information managemen, 19(Spring), 1i. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9123525/

[31] National Institute of Standards and Technology (NIST), *Digital Identity Guidelines*, NIST Special Publication 800-63B, 2020. URL (PDF): https://pages.nist.gov/800-63-3/sp800-63b.html

[32] Microsoft Security Team,"Password guidance: Simplifying your approach" Microsoft, 2021. URL: https://learn.microsoft.com/en-us/microsoft-365/admin/misc/password-policy-recommendations

[33] Verizon, *2023 Data Breach Investigations Report (DBIR)*. URL: https://www.verizon.com/business/resources/reports/dbir/

[34] A. Rahman, M. Rahman, and L. Khan,"Security risks associated with public Wi-Fi: A survey" *IEEE Access*, vol. 9, pp. 87630–87649, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3089803 URL: https://ieeexplore.ieee.org/document/9443358

[35] Kaspersky Lab, *The Dark Side of Public Wi-Fi*, 2022. URL: https://usa.kaspersky.com/resource-center/threats/public-wifi-risks

[36] Proofpoint, *State of the Phish Report*, 2023. URL: https://www.proofpoint.com/us/resources/threat-reports/state-of-phish

[37] R. Ferreira, M. Cruz, and D. Cabral,"Cybersecurity education and phishing susceptibility: An empirical study" *Computers & Security*, vol. 113, 2022. DOI: https://doi.org/10.1016/j.cose.2021.102570 URL: https://www.sciencedirect.com/science/article/pii/S0167404821002885

[38] UNESCO, *Digital Citizenship Education Report*, 2022. URL: https://unesdoc.unesco.org/ark:/48223/pf0000377078

[39] S. Hinduja and J. Patchin, *Cyberbullying Research Center Annual Report*, 2023. URL: https://cyberbullying.org/research

[40] National Initiative for Cybersecurity Education (NICE), *Cybersecurity Workforce Framework*, NIST, 2020. URL: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

[41] T. Sommestad, L. Hallberg, A. Lundholm, and J. Bengtsson,"Training effectiveness to reduce user risk: A systematic review" *Computers & Security*, vol. 87, 2019. DOI: https://doi.org/10.1016/j.cose.2019.101588 URL: https://www.sciencedirect.com/science/article/pii/S0167404819301131

[42] A. Parsons, R. McCormac, N. Butavicius, M. Pattinson, and K. Jerram,"Phishing susceptibility and the impact of repeated training" *Behaviour & Information Technology*, vol. 41, no. 6, 2022. DOI: https://doi.org/10.1080/0144929X.2020.1855299
URL: https://www.tandfonline.com/doi/full/10.1080/0144929X.2020.1855299

[43] R. W. Rogers,"A protection motivation theory of fear appeals and attitude change" *Journal of Psychology*, vol. 91, pp. 93–114, 1975. DOI: https://doi.org/10.1080/00223980.1975.9915803 URL: https://www.tandfonline.com/doi/abs/10.1080/00223980.1975.9915803

[44] M. Workman, W. H. Jones, and D. McCoy,"Human factors in cybersecurity: Examining the role of psychological traits" *Computers in Human Behavior*, vol. 115, 2021. DOI: https://doi.org/10.1016/j.chb.2020.106621 URL: https://www.sciencedirect.com/science/article/pii/S0747563220302895