The North African Journal of Scientific Publishing (NAJSP)
مجلة شمال إفريقيا للنشر العلمي (NAJSP)
E-ISSN: 2959-4820
Volume 4, Issue 2, 2026
Page No: 264-274
Website: https://najsp.com/index.php/home/index
SJIFactor 2024: 5.49 معامل التأثير العربي (AIF) 2025: 0.69 ISI 2024: 0.696

Cybersecurity Awareness in Higher Education: A Literature Review of Educational Practices and Digital Safety

Zakria Mohammed Omar Mrghem[1*], Akram Shebani Ahmad Klella[2]
[1]Computer Science Department, Faculty of Education, Abu-Isa, University of Zawia, Zawia, Libya
https://orcid.org/0009-0005-4986-6520
[2]English Department, Faculty of Education, Abu-Isa, University of Zawia, Zawia, Libya
https://orcid.org/0009-0009-7064-8228

الوعي بالأمن السيبراني في التعليم العالي: مراجعة أدبية للممارسات التعليمية والسلامة الرقمية

زكريا محمد عمر مرغم[1*]، أكرم الشيباني أحمد كليلة[2]
[1]قسم الحاسوب، كلية التربية ابي عيسى، جامعة الزاوية، الزاوية، ليبيا
[2]قسم اللغة الإنجليزية، كلية التربية ابي عيسى، جامعة الزاوية، الزاوية، ليبيا

*Corresponding author: z.mrghem@zu.edu.ly

Received: March 12, 2026	Accepted: April 26, 2026	Published: May 10, 2026

Abstract:
The rapid growth of digital technologies in higher education has increased the importance of cybersecurity awareness and digital safety within universities worldwide. Higher education institutions increasingly rely on online learning platforms, digital communication systems, cloud services, and electronic databases to support teaching, learning, research, and administrative activities. However, this growing dependence on digital technologies has also exposed universities to various cybersecurity threats, including phishing attacks, malware, ransomware, data breaches, and identity theft. Therefore, promoting cybersecurity awareness among students, faculty members, and administrative staff has become essential for protecting institutional systems and ensuring safe digital learning environments.
This literature review examines cybersecurity awareness in higher education by exploring common cybersecurity threats, students' digital behavior, educational practices for cybersecurity awareness, and the role of universities in promoting digital safety. The review also discusses the major challenges facing cybersecurity awareness initiatives in higher education institutions. The findings of the reviewed literature indicate that human behavior and limited cybersecurity awareness remain significant causes of cybersecurity vulnerabilities in universities. The literature further reveals that cybersecurity education, awareness campaigns, workshops, curriculum integration, and practical training programs can positively improve users' cybersecurity knowledge and digital safety practices. The review concludes that universities must adopt comprehensive cybersecurity strategies that combine technical protection measures with continuous cybersecurity education and awareness initiatives. Strengthening cybersecurity awareness and promoting responsible digital citizenship are essential for reducing cybersecurity risks and creating secure digital learning environments in higher education institutions.

Keywords: Cybersecurity Awareness, Higher Education, Digital Safety, Cybersecurity Education, Information Security.

الملخص:
أدى النمو السريع للتقنيات الرقمية في التعليم العالي إلى زيادة أهمية الوعي بالأمن السيبراني والسلامة الرقمية داخل الجامعات على مستوى العالم. وتعتمد مؤسسات التعليم العالي بشكل متزايد على منصات التعلم عبر الإنترنت، وأنظمة الاتصال الرقمية، وخدمات الحوسبة السحابية، وقواعد البيانات الإلكترونية لدعم عمليات التدريس والتعلم والبحث والأنشطة الإدارية. ومع ذلك، فإن هذا الاعتماد المتزايد على التقنيات الرقمية قد عرض الجامعات أيضًا لمجموعة متنوعة من التهديدات السيبرانية، بما في ذلك هجمات التصيّد الاحتيالي، والبرمجيات الخبيثة، وهجمات الفدية، وانتهاكات البيانات، وسرقة الهوية. لذلك أصبح تعزيز الوعي بالأمن السيبراني لدى الطلاب وأعضاء هيئة التدريس والموظفين الإداريين أمرًا ضروريًا لحماية الأنظمة المؤسسية وضمان بيئات تعلم رقمية آمنة. تبحث هذه المراجعة الأدبية في الوعي بالأمن السيبراني في التعليم العالي من خلال استكشاف التهديدات السيبرانية الشائعة، وسلوك الطلاب الرقمي، والممارسات التعليمية لتعزيز الوعي بالأمن السيبراني، ودور الجامعات في تعزيز السلامة الرقمية. كما تناقش المراجعة التحديات الرئيسية التي تواجه مبادرات الوعي بالأمن السيبراني في مؤسسات التعليم العالي. وتشير نتائج الدراسات التي تمت مراجعتها إلى أن السلوك البشري والوعي المحدود بالأمن السيبراني لا يزالان من الأسباب المهمة لضعف الأمن السيبراني في الجامعات. كما تكشف الأدبيات أن التعليم في مجال الأمن السيبراني، وحملات التوعية، وورش العمل، ودمج المناهج الدراسية، وبرامج التدريب العملي يمكن أن تحسن بشكل إيجابي معرفة المستخدمين بالأمن السيبراني وممارسات السلامة الرقمية. وتخلص المراجعة إلى أنه يجب على الجامعات تبني استراتيجيات شاملة للأمن السيبراني تجمع بين إجراءات الحماية التقنية والتثقيف المستمر في مجال الأمن السيبراني ومبادرات التوعية. ويُعد تعزيز الوعي بالأمن السيبراني وتشجيع المواطنة الرقمية المسؤولة أمرًا ضروريًا للحد من المخاطر السيبرانية وخلق بيئات تعلم رقمية آمنة في مؤسسات التعليم العالي.

الكلمات المفتاحية: الوعي بالأمن السيبراني، التعليم العالي، السلامة الرقمية، التعليم في الأمن السيبراني، أمن المعلومات.

Introduction:

The rapid advancement of digital technologies has significantly transformed higher education institutions worldwide. Universities increasingly rely on online learning platforms, cloud computing services, digital communication systems, and electronic databases to support teaching, learning, research, and administrative activities. While these technological developments have improved accessibility, flexibility, and educational efficiency, they have also exposed universities to various cybersecurity threats and digital safety challenges.

Cybersecurity has become a critical issue in higher education due to the growing number of cyberattacks targeting educational institutions. Universities store large amounts of sensitive information, including students' personal data, academic records, financial information, and research materials, making them attractive targets for cybercriminals. Common cybersecurity threats in higher education include phishing attacks, malware, ransomware, identity theft, data breaches, and unauthorized access to institutional systems. These threats can negatively affect students, faculty members, and university infrastructures, leading to financial losses, privacy violations, and disruptions in educational activities. In this digital era, cybersecurity awareness plays a vital role in protecting individuals and institutions from cyber risks.

Cybersecurity awareness refers to individuals' understanding of cyber threats, safe online practices, and responsible digital behavior. In higher education, promoting cybersecurity awareness among students, teachers, and university staff is essential to ensure safe and secure digital learning environments. Educational institutions are increasingly implementing awareness programs, cybersecurity training, workshops, and digital safety policies to improve users' knowledge and reduce cybersecurity vulnerabilities. Despite the increasing attention given to cybersecurity in higher education, many students and university users continue to demonstrate limited awareness of digital safety practices. Weak password management, unsafe internet behavior, lack of knowledge about phishing attacks, and insufficient cybersecurity training remain common issues among university communities. These challenges highlight the importance of reviewing existing literature to better understand current educational practices, cybersecurity awareness strategies, and digital safety concerns in higher education institutions.

Therefore, this literature review aims to examine cybersecurity awareness in higher education by exploring educational practices used to promote digital safety and analyzing the major cybersecurity challenges faced by universities. The paper also reviews previous studies related to cybersecurity awareness and discusses the role of higher education institutions in creating secure digital learning environments. Through this review, the study seeks to provide a comprehensive understanding of the importance of cybersecurity education and its contribution to improving digital safety in higher education.

Concept of Cybersecurity and Cybersecurity Awareness:

Cybersecurity has become an essential component of modern digital society due to the increasing dependence on information technology and internet-based systems. It refers to the protection of computer systems, networks, software, and data from cyber threats, unauthorized access, damage, or attacks. According to Stallings and Brown (2018), cybersecurity involves the technologies, processes, and practices designed to protect digital systems and sensitive information from cyberattacks. Similarly, Von Solms and Van Niekerk (2013) explained that cybersecurity is not limited to technical protection mechanisms but also includes human behavior, organizational policies, and risk management strategies.

The rapid growth of digital technologies in education, business, healthcare, and government sectors has increased the importance of cybersecurity worldwide. Higher education institutions, in particular, have become highly dependent on digital learning environments, cloud services, online communication platforms, and electronic databases. However, this digital transformation has also exposed universities to various cybersecurity risks, including phishing attacks, malware, ransomware, data breaches, and identity theft (Al-Janabi & Al-Shourbaji, 2016). As a result, universities must adopt effective cybersecurity measures to protect institutional systems and users' personal information. Cybersecurity awareness refers to individuals' knowledge, understanding, and attitudes regarding cyber threats and safe online behavior. It involves recognizing cybersecurity risks and applying appropriate practices to reduce vulnerabilities and maintain digital safety. Parsons et al. (2017) stated that cybersecurity awareness includes users' ability to identify cyber threats, understand security policies, and engage in responsible digital behavior. In educational environments, cybersecurity awareness helps students, teachers, and staff members protect themselves and institutional systems from cyber risks. Researchers have emphasized that human factors are among the most significant causes of cybersecurity incidents. Many cyberattacks succeed because users lack sufficient awareness of digital safety practices such as password security, email verification, and data protection. According to Kruger and Kearney (2006), cybersecurity awareness is essential because even advanced technical security systems cannot fully protect organizations if users demonstrate unsafe online behavior. Therefore, educational institutions must focus on increasing cybersecurity awareness alongside implementing technical security measures. In higher education, cybersecurity awareness has become increasingly important due to the widespread use of e-learning platforms, online assessments, digital libraries, and virtual communication tools (Bada et al., 2019). Students and university staff frequently access institutional systems through personal devices and public networks, which may increase exposure to cyber threats. Consequently, universities are encouraged to develop cybersecurity awareness programs, workshops, training sessions, and digital safety campaigns to educate users about secure online practices.

Cybersecurity in Higher Education:

The increasing integration of digital technologies in higher education has transformed the way universities conduct teaching, learning, research, and administrative activities. Educational institutions now rely heavily on online learning platforms, cloud computing, digital communication systems, and electronic databases to support academic operations. While these technologies provide greater accessibility, flexibility, and efficiency, they also expose universities to significant cybersecurity risks and digital threats (Brooks et al., 2018).

Higher education institutions are considered attractive targets for cybercriminals because they store large amounts of sensitive information, including students' personal data, financial records, academic documents, and research materials. In addition, universities often maintain open and decentralized digital environments that allow thousands of users to access institutional systems through multiple devices and networks. According to Educause (2021), the openness of university networks and the extensive use of online technologies increase the vulnerability of higher education institutions to cyberattacks. One of the major cybersecurity challenges facing universities is the increasing number of phishing attacks, malware infections, ransomware incidents, and data breaches. Phishing attacks are among the most common threats in educational environments because students and staff frequently use email communication for academic purposes. Cybercriminals often exploit users' lack of cybersecurity awareness to gain unauthorized access to institutional systems and confidential information (Al-Janabi & Al-Shourbaji, 2016). Similarly, ransomware attacks have become a growing concern in higher education, as attackers may encrypt institutional data and demand financial payments to restore access. The widespread adoption of e-learning systems and virtual learning environments has also contributed to cybersecurity concerns in higher education. Learning Management Systems (LMS), video conferencing platforms, and online assessment tools require students and faculty members to share personal information and access digital services remotely.

While these systems enhance educational accessibility, they may also create security vulnerabilities if institutions fail to implement strong cybersecurity measures (Ismail et al., 2022). Weak passwords, insecure networks, and inadequate security configurations can increase the risk of unauthorized access and cyberattacks. Human factors represent another important issue in university cybersecurity. Many cybersecurity incidents occur because users lack sufficient awareness of safe online practices. Students and staff members may unintentionally expose institutional systems to cyber risks through poor password management, unsafe internet behavior, or failure to recognize phishing emails. According to Parsons et al. (2017), cybersecurity awareness among users plays a critical role in reducing security vulnerabilities and improving institutional protection against cyber threats. To address these challenges, universities are increasingly implementing cybersecurity policies, awareness campaigns, and training programs to improve digital safety (Bada et al., 2019). Educational institutions are also investing in technical security measures such as firewalls, encryption systems, multi-factor authentication, and network monitoring tools. Furthermore, cybersecurity education has become an important part of university strategies aimed at promoting responsible digital behavior and protecting institutional resources.

Common Cybersecurity Threats in Universities:

Universities and higher education institutions increasingly face a wide range of cybersecurity threats due to their extensive use of digital technologies and open network environments. Educational institutions store valuable information, including students' personal data, financial records, academic research, and institutional databases, making them attractive targets for cybercriminals (Brooks et al., 2018). The growing dependence on online learning systems, cloud services, and digital communication platforms has further increased cybersecurity vulnerabilities in higher education.

One of the most common cybersecurity threats in universities is phishing attacks. Phishing refers to fraudulent attempts to obtain sensitive information such as usernames, passwords, and financial details by pretending to be a trustworthy source. Attackers often send fake emails or messages that appear to come from university departments, instructors, or administrative offices. Students and staff members who lack cybersecurity awareness may unintentionally disclose confidential information or click malicious links that compromise institutional systems (Al-Janabi & Al-Shourbaji, 2016). Phishing attacks are particularly dangerous because they rely on human error rather than technical system weaknesses. Malware is another significant cybersecurity threat affecting universities. Malware refers to malicious software designed to damage computer systems, steal data, or gain unauthorized access to networks. Common forms of malware include viruses, worms, spyware, and Trojan horses. Cybercriminals may distribute malware through infected email attachments, unsafe websites, or unauthorized software downloads. According to Stallings and Brown (2018), malware attacks can disrupt university operations, damage digital infrastructure, and compromise sensitive institutional data. Ransomware attacks have also become increasingly common in higher education institutions. Ransomware is a type of malware that encrypts files or systems and demands payment in exchange for restoring access (Ismail et al., 2022). Universities are particularly vulnerable to ransomware because they manage large amounts of valuable data and rely heavily on digital systems for academic activities. Successful ransomware attacks may interrupt online learning, administrative operations, and research activities, causing serious financial and operational consequences

Data breaches represent another major cybersecurity concern in universities. A data breach occurs when unauthorized individuals gain access to confidential information stored within institutional systems. Educational institutions often maintain large databases containing personal, academic, and financial information, which can become targets for hackers. Data breaches may result from weak passwords, software vulnerabilities, insider threats, or phishing attacks. According to Von Solms and Van Niekerk (2013), data breaches can lead to privacy violations, financial losses, and reputational damage for universities. Identity theft is also a growing issue in higher education environments. Cybercriminals may steal personal information such as student identification numbers, passwords, or financial data to commit fraud or gain unauthorized access to university systems. Students are particularly vulnerable because they frequently use online services, social media platforms, and public internet connections (Parsons et al., 2017). Weak password management and poor cybersecurity awareness can increase the risk of identity theft among university users.

In addition, social engineering attacks pose serious cybersecurity risks in universities. Social engineering involves manipulating individuals into revealing confidential information or performing actions that compromise security (Bada et al., 2019). Attackers may impersonate university staff, technical support personnel, or trusted organizations to deceive students and employees. These attacks exploit human psychology rather than technical vulnerabilities, making cybersecurity awareness and digital literacy essential for prevention.

Educational Practices for Cybersecurity Awareness:

Educational practices for cybersecurity awareness have become increasingly important in higher education institutions due to the rapid growth of digital technologies and cyber threats. Universities are adopting various educational strategies and awareness programs to help students, faculty members, and administrative staff understand cybersecurity risks and develop safe online behaviors (Bada et al., 2019). Effective cybersecurity education not only improves users' knowledge of digital threats but also contributes to creating secure digital learning environments within educational institutions.

One of the most common educational practices used to promote cybersecurity awareness is cybersecurity training programs. Universities frequently organize training sessions and workshops to educate users about common cyber threats such as phishing attacks, malware, ransomware, and identity theft. These programs aim to teach participants how to recognize suspicious online activities, create strong passwords, protect personal information, and safely use digital platforms. According to Parsons et al. (2017), regular cybersecurity training can significantly improve users' awareness and reduce risky online behavior. Awareness campaigns are another effective educational strategy implemented in higher education institutions. Universities often use emails, posters, webinars, social media content, and online announcements to spread information about cybersecurity risks and safe digital practices. These campaigns help remind students and staff about the importance of digital safety and encourage them to follow institutional cybersecurity policies. Bada et al. (2019) emphasized that awareness campaigns are essential for promoting long-term behavioral change and strengthening cybersecurity culture within organizations.

Integrating cybersecurity education into university curricula has also become an important educational practice. Many universities now include cybersecurity topics in computer science, information technology, and general education courses. Teaching cybersecurity concepts in academic programs allows students to develop knowledge about digital safety, cyber ethics, data protection, and responsible technology use. According to Alharbi et al. (2021), incorporating cybersecurity education into higher education curricula helps students acquire practical skills and prepares them to face cybersecurity challenges in both academic and professional environments. Simulation exercises and practical learning activities are increasingly used to enhance cybersecurity awareness in universities. For example, some institutions conduct simulated phishing attacks to test users' ability to identify fraudulent emails and malicious links (Kruger & Kearney, 2006). These practical exercises provide hands-on experience and help users understand real-world cyber threats. Experiential learning methods are considered highly effective because they encourage active participation and improve the application of cybersecurity knowledge in daily digital activities.

Online learning platforms and digital resources also play an important role in cybersecurity education. Universities use Learning Management Systems (LMS), video tutorials, online courses, and educational websites to provide cybersecurity training and awareness materials. Online educational resources offer flexible access to cybersecurity information and allow students to learn at their own pace. Furthermore, digital platforms can be regularly updated to address emerging cybersecurity threats and evolving technological risks (Ismail et al., 2022). Another important educational practice involves promoting digital citizenship and responsible online behavior (Ribble, 2015). Universities encourage students and staff to follow ethical and secure digital practices such as respecting privacy, protecting sensitive information, avoiding suspicious websites, and responsibly using social media Developing digital responsibility helps reduce cybersecurity vulnerabilities caused by human error and unsafe online behavior.

Students' Cybersecurity Awareness and Digital Behavior:

Students' cybersecurity awareness and digital behavior have become important concerns in higher education due to the increasing use of digital technologies and online learning environments. University students regularly access educational platforms, social media applications, email services, cloud storage systems, and online communication tools as part of their academic and personal activities (Al-Janabi & Al-Shourbaji, 2016). While digital technologies provide many educational benefits, unsafe online behavior and limited cybersecurity awareness can expose students and educational institutions to significant cyber threats.

Cybersecurity awareness refers to students' understanding of cyber threats, digital safety practices, and responsible online behavior. Students with strong cybersecurity awareness are more likely to recognize phishing emails, create secure passwords, protect personal information, and avoid suspicious online activities. According to Parsons et al. (2017), cybersecurity awareness plays a critical role in reducing human-related cybersecurity vulnerabilities because many cyberattacks succeed due to users' unsafe digital practices rather than technical system weaknesses. One of the most common issues related to students' digital behavior is weak password management. Many students use simple passwords, reuse the same passwords across multiple accounts, or share passwords with others,

increasing the risk of unauthorized access to personal and institutional systems. Weak password practices make university accounts vulnerable to hacking, identity theft, and data breaches (Kruger & Kearney, 2006). Therefore, students must be educated about the importance of strong passwords and multi-factor authentication to improve digital security.

Phishing attacks also significantly affect students in higher education. Cybercriminals often target students through fake emails, fraudulent websites, and deceptive online messages designed to steal personal information or login credentials. Students who lack cybersecurity awareness may unintentionally click malicious links or download harmful files, leading to malware infections and compromised accounts. According to Bada et al. (2019), educational awareness programs are essential to help students identify phishing attempts and practice safe online communication. Social media usage represents another important aspect of students' digital behavior. University students extensively use social networking platforms for communication, entertainment, and academic collaboration. However, oversharing personal information on social media can increase exposure to cyber threats such as identity theft, cyberbullying, and social engineering attacks. Researchers have emphasized that students should understand privacy settings, digital footprints, and responsible online behavior to protect their personal information and maintain digital safety (Ribble, 2015).

In addition, students frequently use public Wi-Fi networks and personal devices to access university systems and educational resources. Although these technologies provide convenience and accessibility, insecure networks and poorly protected devices can expose users to cybersecurity risks. Malware attacks, unauthorized access, and data interception are more likely to occur when students use unprotected internet connections or outdated software systems (Stallings & Brown, 2018). Consequently, universities should encourage students to adopt safe browsing practices and regularly update their devices and security software. Digital behavior is also influenced by students' level of digital literacy and cybersecurity education. Students who receive cybersecurity training and awareness instruction are generally more capable of practicing safe online behavior and responding effectively to cyber threats (Alharbi et al., 2021). Educational institutions play an important role in promoting responsible digital citizenship by integrating cybersecurity education into academic programs and awareness campaigns.

Challenges of Cybersecurity Awareness in Higher Education:

Higher education institutions face numerous challenges in promoting cybersecurity awareness and ensuring digital safety among students, faculty members, and administrative staff. The rapid expansion of digital technologies, online learning systems, and internet-based educational services has increased universities' exposure to cyber threats and security vulnerabilities (Brooks et al., 2018). Although universities continue to invest in cybersecurity measures and awareness programs, several organizational, technical, and human-related challenges limit the effectiveness of cybersecurity awareness initiatives.

One of the primary challenges is the lack of adequate cybersecurity awareness among university users. Many students and staff members possess limited knowledge about cyber threats, safe online practices, and digital security policies. As a result, users may engage in risky online behavior such as using weak passwords, clicking suspicious links, downloading unauthorized software, or sharing sensitive information through insecure platforms. According to Parsons et al. (2017), human behavior remains one of the weakest aspects of cybersecurity because users often fail to recognize or respond appropriately to cyber threats. Another significant challenge is the rapid evolution of cyber threats and attack techniques (Bada et al., 2019). Cybercriminals continuously develop new methods to exploit technological vulnerabilities and deceive users through phishing attacks, ransomware, malware, and social engineering. Universities may struggle to keep cybersecurity awareness programs updated in response to emerging threats. Consequently, outdated training materials and infrequent awareness campaigns may reduce users' ability to recognize modern cybersecurity risks.

Limited financial and technical resources also represent major obstacles for higher education institutions. Some universities, particularly in developing countries, may lack sufficient funding to implement advanced cybersecurity infrastructure, regular training programs, and specialized security teams. Inadequate investment in cybersecurity education and digital protection systems can increase institutional vulnerability to cyberattacks and data breaches (Al-Janabi & Al-Shourbaji, 2016). Furthermore, smaller institutions may experience difficulties maintaining updated security technologies and monitoring digital threats effectively. The open and decentralized nature of university environments creates additional cybersecurity challenges. Universities encourage collaboration, academic freedom, and unrestricted access to information, which often requires flexible and widely accessible digital networks. However, this openness may increase security vulnerabilities because thousands of users connect to institutional systems through personal devices, remote networks, and public internet

connections. According to Esucause (2021), balancing accessibility and cybersecurity protection remains one of the most complex issues in higher education cybersecurity management.

Another challenge involves insufficient participation and engagement in cybersecurity awareness programs. Many students and staff members may view cybersecurity training as unimportant, repetitive, or unrelated to their academic responsibilities. Low motivation and lack of user engagement can reduce the effectiveness of awareness campaigns and educational initiatives. Researchers have emphasized that awareness programs should be interactive, practical, and continuously reinforced to encourage long-term behavioral change (Kruger & Kearney, 2006).

Digital literacy differences among university users also contribute to cybersecurity awareness challenges. Students and staff possess varying levels of technological knowledge and digital skills, which may affect their ability to understand cybersecurity concepts and apply safe online practices. Users with limited digital literacy are generally more vulnerable to phishing attacks, identity theft, and unsafe internet behavior (Ribble, 2015). Therefore, universities must design cybersecurity awareness programs that address the needs of users with different technological backgrounds and skill levels. Additionally, the increasing use of personal devices and remote learning technologies has complicated cybersecurity management in higher education. Students frequently use smartphones, laptops, and tablets to access university systems and online learning platforms. While these technologies improve flexibility and accessibility, they may also expose institutions to security risks if devices are not properly secured or regularly updated (Ismail et al., 2022). Remote learning environments further increase cybersecurity concerns because users often connect through home networks or public Wi-Fi systems that may lack strong security protections.

Role of Universities in Promoting Digital Safety:

Universities play a significant role in promoting digital safety and strengthening cybersecurity awareness among students, faculty members, and administrative staff. As higher education institutions increasingly rely on digital technologies for teaching, learning, research, and communication, universities are responsible for creating secure digital environments that protect users and institutional systems from cyber threats (Brooks et al., 2018). Promoting digital safety has become an essential component of university policies and educational strategies in the modern digital era.

One of the primary responsibilities of universities is providing cybersecurity education and awareness programs. Educational institutions organize workshops, seminars, online training sessions, and awareness campaigns to educate students and staff about cyber threats and safe online practices. These programs focus on important topics such as password security, phishing detection, safe internet usage, data protection, and responsible digital behavior. According to Bada et al. (2019), continuous cybersecurity awareness initiatives can improve users' understanding of digital risks and encourage safer online practices within educational communities.

Universities also contribute to digital safety by integrating cybersecurity education into academic curricula. Many higher education institutions include cybersecurity concepts in computer science, information technology, and general education courses to prepare students for the digital world. Teaching cybersecurity principles helps students develop technical knowledge, digital responsibility, and awareness of online threats. Alharbi et al. (2021) emphasized that integrating cybersecurity education into university curricula is essential for developing students' cybersecurity competencies and promoting long-term digital safety awareness. In addition to educational initiatives, universities are responsible for implementing institutional cybersecurity policies and technical protection measures. Educational institutions establish regulations regarding password management, data privacy, network access, and acceptable technology use to reduce cybersecurity risks. Universities also invest in digital security technologies such as firewalls, encryption systems, antivirus software, and multi-factor authentication to protect institutional networks and sensitive information (Stallings & Brown, 2018). These technical measures help strengthen digital infrastructure and reduce the likelihood of cyberattacks.

Another important role of universities is promoting a culture of responsible digital citizenship. Universities encourage students and staff to use technology ethically, respect online privacy, protect confidential information, and avoid harmful digital behavior. According to Ribble (2015), digital citizenship education supports safe and responsible participation in digital environments by promoting ethical technology use and awareness of online risks. Developing responsible digital behavior is particularly important because human error and unsafe online practices often contribute to cybersecurity incidents. Universities also support digital safety through continuous monitoring and incident response strategies. Many institutions establish information technology departments and cybersecurity teams responsible for identifying vulnerabilities, responding to cyber incidents, and maintaining institutional security systems (Educause, 2021). These teams help universities manage cybersecurity risks, monitor suspicious activities, and provide technical support to users. Effective

cybersecurity management contributes to maintaining stable and secure digital learning environments (Ismail et al., 2022). Collaboration with governmental organizations, cybersecurity experts, and technology companies further enhances universities' efforts to promote digital safety. Partnerships with external organizations provide institutions with updated cybersecurity knowledge, training resources, and technological support.

Previous Studies:

Several previous studies have examined cybersecurity awareness, cyber threats, and digital safety practices in higher education institutions. Researchers have focused on understanding the level of cybersecurity awareness among university students and staff, identifying common cyber threats, and evaluating the effectiveness of cybersecurity education programs and institutional strategies.

Al-Janabi and Al-Shourbaji (2016) conducted a study on cybersecurity awareness in educational environments in the Middle East. The study found that many students and university users lacked sufficient knowledge about cybersecurity risks and safe online practices. The researchers emphasized the importance of implementing cybersecurity awareness programs and educational initiatives to improve digital safety in higher education institutions. The study also highlighted that human behavior remains one of the major causes of cybersecurity vulnerabilities in universities. Similarly, Parsons et al. (2017) examined the role of human factors in information security by developing the Human Aspects of Information Security Questionnaire (HAIS-Q). Their findings showed that users' cybersecurity awareness significantly influences online behavior and institutional security. The study concluded that improving users' knowledge of password security, email safety, and internet usage could reduce cybersecurity risks in organizational environments, including universities.

Bongiovanni (2019) conducted a systematic literature review on information security management in higher education institutions. The study revealed that universities are increasingly becoming targets of cyberattacks because of their open digital environments and extensive use of online technologies. The review identified major cybersecurity challenges such as phishing attacks, data breaches, weak security governance, and insufficient cybersecurity awareness among university communities. The author recommended that universities strengthen institutional cybersecurity policies and awareness initiatives to improve digital safety. Bada et al. (2019) investigated the effectiveness of cybersecurity awareness campaigns and found that many awareness programs fail to produce long-term behavioral change because they focus mainly on information delivery rather than user engagement and practical learning experiences. The researchers emphasized the importance of interactive educational strategies and continuous cybersecurity training to improve users' digital behavior and security awareness.

Alqahtani (2022) explored factors affecting cybersecurity awareness among university students. The study demonstrated that cybersecurity education, digital literacy, and training programs positively influence students' cybersecurity awareness and online behavior. The findings also indicated that students with stronger cybersecurity knowledge were more capable of identifying phishing attempts, protecting personal information, and practicing safe internet usage. More recently, Ismail et al. (2022) reviewed cybersecurity challenges in higher education institutions and identified several major threats, including ransomware attacks, phishing emails, malware infections, and weak password management. The study emphasized that universities should combine technical security measures with cybersecurity education and awareness programs to reduce institutional vulnerabilities and strengthen digital protection.

A recent study by Afolalu and Tsoeu (2025) systematically reviewed emerging cybersecurity trends and challenges in higher education institutions. The researchers found that phishing attacks, ransomware, and data breaches continue to represent major cybersecurity threats in universities. The study also emphasized that limited cybersecurity awareness, fragmented institutional policies, and technological gaps contribute significantly to cybersecurity vulnerabilities in higher education. The authors recommended institution-wide cybersecurity awareness strategies and stronger collaboration among universities to improve digital safety. Amzeyeva and Zhumabayeva (2025) conducted a systematic literature review focusing on cybersecurity awareness among students. Their study revealed that students frequently encounter cyber threats such as phishing, social engineering, identity theft, and cyberbullying. Baleid and Abdullah (2026) reviewed cybersecurity threats and mitigation strategies in higher education institutions. Their findings found that interactive learning methods, gamification, and practical cybersecurity training significantly improve students' awareness and digital safety skills. The study recommended integrating cybersecurity education into academic curricula to develop a stronger cybersecurity culture among students.

Discussion:

The reviewed literature demonstrates that cybersecurity awareness has become an essential issue in higher education due to the rapid digital transformation of universities and the increasing dependence on online technologies. Educational institutions rely heavily on digital platforms, cloud services, virtual

learning environments, and electronic communication systems to support teaching, learning, research, and administrative activities (Brooks et al., 2018). While these technologies provide numerous educational benefits, they also expose universities to various cybersecurity threats and digital safety challenges.

One of the major findings in the literature is that human behavior remains a significant factor contributing to cybersecurity vulnerabilities in higher education institutions. Several studies emphasized that students and staff members often demonstrate insufficient cybersecurity awareness and unsafe digital behavior, including weak password management, failure to recognize phishing attacks, and risky internet practices (Parsons et al., 2017). This finding supports the argument that technical protection measures alone are not enough to ensure cybersecurity in educational environments. Universities must also focus on educating users and promoting responsible digital behavior. The reviewed studies consistently identified phishing attacks, malware infections, ransomware attacks, data breaches, and social engineering as the most common cybersecurity threats in universities (Ismail et al., 2022). These threats are particularly dangerous because higher education institutions maintain open and decentralized digital environments that allow large numbers of users to access institutional systems through personal devices and remote networks. As noted by Bongiovanni (2019), the openness of university systems creates additional cybersecurity risks and makes higher education institutions attractive targets for cybercriminals.

Another important finding is the significant role of cybersecurity education and awareness programs in improving digital safety. The literature revealed that cybersecurity training sessions, workshops, awareness campaigns, and curriculum integration positively influence students' cybersecurity knowledge and online behavior (Alharbi et al., 2021). Educational initiatives help users recognize cyber threats, protect personal information, and adopt safe online practices. However, some studies argued that traditional awareness campaigns may not always lead to long-term behavioral change because they often focus on information delivery rather than interactive learning and practical application (Bada et al., 2019). The discussion of previous studies also highlights the importance of integrating cybersecurity education into university curricula. Researchers emphasized that cybersecurity awareness should not be limited to technical disciplines such as computer science and information technology (Ribble, 2015). Instead, all university students should receive basic cybersecurity education because digital technologies are widely used across all academic fields. Integrating cybersecurity concepts into higher education curricula can help students develop digital literacy, responsible online behavior, and awareness of cybersecurity risks.

Despite increasing efforts to improve cybersecurity awareness, universities continue to face several challenges. Limited financial resources, rapid technological changes, insufficient user participation, and varying levels of digital literacy reduce the effectiveness of cybersecurity initiatives (Al-Janabi & Al-Shourbaji, 2016). In addition, many universities struggle to balance open academic environments with strict cybersecurity protections. Educational institutions must therefore adopt comprehensive cybersecurity strategies that combine technical security measures, institutional policies, awareness programs, and continuous training (Afolalu & Tsoeu, 2025). Furthermore, the reviewed literature suggests that cybersecurity awareness should be viewed as a continuous educational process rather than a single training activity. Cyber threats constantly evolve, requiring universities to regularly update awareness programs and digital safety practices. Continuous cybersecurity education can help institutions respond more effectively to emerging cyber threats and improve institutional resilience against cyberattacks.

Recommendations:

Based on the reviewed literature, several recommendations can be proposed to improve cybersecurity awareness and promote digital safety in higher education institutions.

First, universities should provide regular cybersecurity awareness programs and training sessions for students, faculty members, and administrative staff. These programs should focus on common cyber threats such as phishing attacks, malware, ransomware, password security, and safe internet practices. Continuous training can help users develop the knowledge and skills needed to recognize and respond to cybersecurity risks effectively. Second, higher education institutions should integrate cybersecurity education into university curricula across different academic disciplines. Cybersecurity awareness should not be limited to computer science and information technology students only. All students should receive basic cybersecurity education because digital technologies are widely used in all fields of study and professional environments. Third, universities should strengthen institutional cybersecurity policies and digital protection systems. Educational institutions should implement strong password requirements, multi-factor authentication, secure network systems, data encryption technologies, and regular software updates to improve digital security and reduce cybersecurity vulnerabilities. Fourth, universities should promote a culture of responsible digital citizenship among students and staff

members. Educational institutions should encourage ethical technology use, respect for online privacy, protection of personal information, and responsible online communication. Promoting positive digital behavior can help reduce cybersecurity incidents caused by human error and unsafe online practices. Fifth, universities should use interactive and practical learning methods to improve cybersecurity awareness. Simulation exercises, phishing detection activities, workshops, and hands-on cybersecurity training can help users apply cybersecurity knowledge in real-life digital situations more effectively than traditional awareness campaigns alone. Sixth, higher education institutions should increase collaboration with cybersecurity experts, governmental organizations, and technology companies to strengthen cybersecurity practices and stay informed about emerging cyber threats. External partnerships can provide universities with updated cybersecurity knowledge, technical support, and professional training opportunities.

Conclusion:

Cybersecurity awareness has become a critical issue in higher education due to the rapid expansion of digital technologies and the increasing dependence on online learning environments, digital communication systems, and electronic information management. Universities face growing cybersecurity challenges as cybercriminals continue to target educational institutions through phishing attacks, malware, ransomware, data breaches, and social engineering techniques. The reviewed literature demonstrates that higher education institutions are particularly vulnerable because of their open digital environments, large user populations, and extensive use of internet-based technologies.

The literature also highlights that human behavior plays a major role in cybersecurity vulnerabilities within universities. Many students and staff members continue to demonstrate limited cybersecurity awareness and unsafe digital practices, including weak password management, poor recognition of phishing attempts, and risky online behavior. These findings indicate that technical security systems alone are insufficient to protect higher education institutions from cyber threats. Effective cybersecurity protection requires both technological measures and continuous cybersecurity education. Furthermore, the reviewed studies emphasize the importance of educational practices in promoting cybersecurity awareness and digital safety. Cybersecurity training programs, awareness campaigns, workshops, curriculum integration, and practical learning activities have been identified as effective strategies for improving users' cybersecurity knowledge and encouraging responsible online behavior. Universities play a vital role in promoting digital safety by implementing institutional cybersecurity policies, providing educational resources, and fostering a culture of responsible digital citizenship. Despite ongoing efforts to strengthen cybersecurity awareness, higher education institutions continue to face several challenges, including rapid technological changes, limited resources, varying levels of digital literacy, and insufficient participation in awareness programs. These challenges highlight the need for comprehensive cybersecurity strategies that combine technical protection systems, institutional support, cybersecurity education, and continuous awareness initiatives.

Cybersecurity awareness is essential for creating secure digital learning environments and protecting higher education institutions from evolving cyber threats. Universities must continue investing in cybersecurity education, strengthening institutional policies, and encouraging safe digital behavior among students and staff. By promoting cybersecurity awareness and digital responsibility, higher education institutions can improve digital safety, reduce cybersecurity risks, and support the effective and secure use of technology in modern education.

References:

1. Afolalu, O., & Tsoeu, M. S. (2025). Cybersecurity in higher education institutions: A systematic review of emerging trends, challenges and solutions. Future Internet, 17(12), 575. https://doi.org/10.3390/fi17120575
2. Alharbi, F., Walters, R., & Wills, G. (2021). Cybersecurity awareness and education in higher education institutions: A review. International Journal of Information and Education Technology, 11(5), 215–221. https://doi.org/10.18178/ijiet.2021.11.5.1516
3. Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the Middle East. Journal of Information & Knowledge Management, 15(1), 1650007. https://doi.org/10.1142/S0219649216500076
4. Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589
5. Amzeyeva, A. A., & Zhumabayeva, A. E. (2025). Cybersecurity awareness among students: A systematic literature review and PRISMA-based analysis. Gumilyov Journal of Pedagogy, 152(3), 126–144. https://doi.org/10.32523/3080-1710-2025-152-3-126-144
6. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv Preprint arXiv:1901.02672. https://arxiv.org/abs/1901.02672

7. Baleid, H. M., & Abdullah, M. F. (2026). Cybersecurity in higher education: A systematic review of threats, challenges, and mitigation strategies. Journal of Science and Technology, 31(1). https://doi.org/10.20428/jst.v31i1.3563
8. Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Computers & Security, 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003
9. Brooks, D. C., Grajek, S., & Lang, L. (2018). Information security strategy and practices in higher education. EDUCAUSE Review. https://er.educause.edu/articles/2018/10/information-security-strategy-and-practices-in-higher-education
10. Educause. (2021). Top IT issues, 2021: Emerging from the pandemic. EDUCAUSE Review. https://er.educause.edu/articles/2021/1/top-it-issues-2021-emerging-from-the-pandemic
11. Ismail, N. A., AlMazroi, A., & Ahamed, F. (2022). Cybersecurity challenges in higher education institutions: A review study. International Journal of Information and Education Technology, 12(3), 210–216. https://doi.org/10.18178/ijiet.2022.12.3.1608
12. 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
13. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). 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. Ribble, M. (2015). Digital citizenship in schools: Nine elements all students should know (3rd ed.). International Society for Technology in Education.
15. Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson.
16. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004