STM JOURNALS

International Journal of
Wireless Security and Networks

ISSN: 2584-0703
Volume 2, Issue 1, 2024
January–June
DOI (Journal): 10.37591/IJWSN

https://journals.stmjournals.com/ijwsn

Review IJWSN

A Roadmap to Digital Path: Empowering College Students in Cybersecurity

Anand Raj I.[1,*], R. Vidya[2]

Abstract

A cybersecurity area that focuses on college students, digital citizens of our time, who play an important role in determining the future of cybersecurity. It focuses on the unique challenges college students face, from identity theft to cyber and sensitive data security. This report examines best practices and methods for building college students' online barriers and underscores the need for digital literacy, literacy, and personal responsibility in an era of increasing and disappearing online risk. This shows the responsibility of universities to create a culture of cyber security among students. Looking forward, this article discusses possible approaches to online safety for college students. It covers a dynamic view of cyber threats, new technologies, and the need for adaptation and innovation. It describes the activities needed to educate the next generation of professionals with the knowledge and skills to navigate the cybersecurity environment, with a focus on education, awareness programs, and internships. In summary, this article explores the dynamic relationship between college students and cybersecurity, highlighting the challenges they face, best practices for protecting their digital worlds, and progress in this important sector.

Keywords: Cybersecurity, information security, data protection, online privacy, security policies

INTRODUCTION

Especially in the digital revolution and hyper-connected age, the importance of internet safety for college students has never been greater. But it also brought an era of unprecedented cyber risks, data breaches, and cyber vulnerabilities. The digital world has created great potential for learning, collaboration, and communication. College students should be well versed in cybersecurity concepts as they are the main targets and defenders of the digital world. College students navigate the vast and dynamic network of online services, platforms, and devices known as the "digital landscape". Internet use permeates all aspects of life, from social networking and managing personal finances to academic research and distance education. But this widespread involvement carries its risks, as attackers use digital flaws to compromise security, privacy, and data. This study aims to explain the important role of cyber security in the lives of university students by addressing the many challenges they face in the digital world. This shows the great need for cybersecurity training and methods suited to the characteristics and weaknesses of each individual. Especially in the digital revolution and hyper-connected age, the importance of internet safety for college students has never been greater. But it also brought an era of unprecedented cyber risks, data breaches, and cyber vulnerabilities. The digital world has created great potential for learning, collaboration, and communication. College students should be well versed in cybersecurity concepts as they are the main targets and defenders of the digital world. College students navigate the vast and

***Author for Correspondence**
Anand Raj I.
E-mail: ammayesuraja75@gmail.com

[1]Research Scholar, Department of Computer Science, St. Joseph's College of Arts & Science (Autonomous), Cuddalore, Tamil Nadu, India
[2]Research Supervisor and Assistant Professor, Department of Computer Science, St. Joseph's College of Arts & Science (Autonomous), Cuddalore, Tamil Nadu, India

Received Date: March 26, 2024
Accepted Date: March 28, 2024
Published Date: May 01, 2024

Citation: Anand Raj I., R. Vidya. A Roadmap to Digital Path: Empowering College Students in Cybersecurity. International Journal of Wireless Security and Networks. 2024; 2(1): 30–39p.

© STM Journals 2024. All Rights Reserved

dynamic network of online services, platforms, and devices known as the "digital landscape". Internet use permeates all aspects of life, from social networking and managing personal finances to academic research and distance education. But this widespread involvement carries its risks, as attackers use digital flaws to compromise security, privacy, and data. This study aims to explain the important role of cyber security in the lives of university students by addressing the many challenges they face in the digital world. This shows the great need for cybersecurity training and methods suited to the characteristics and weaknesses of each individual.

LITERATURE REVIEW

To meet the requirements of the National Cyber Security Strategic Plan (NCSP), cybersecurity skills, capabilities, and knowledge must be integrated and coordinated across the program [1]. In general, cybersecurity aims to educate people about security standards and appropriate behavior so that they can treat unusual or extraordinary situations with appropriate skepticism [2]. All aspects of enterprise information security are directly affected by human factors, and people are the weakest link in the chain of protection of the information security system [3]. It has been repeatedly said that different economies suffer significant losses due to various disasters, including infrastructure sectors such as transport, health, energy, and water supply [4]. The Cybersecurity Master's program addresses today's security issues and provides future security professionals with fundamental technical knowledge and skills [5]. Predicting behavioral intentions and cognitive understanding of cybersecurity activities [6]. Due to the anonymity of the internet, fees can be determined and sent [7]. Any informal activity that people perform to achieve health goals outside of the clinical setting, without supervision or even contact with a health professional, is considered self-care [8]. Participating in these cybersecurity communities of practice can help students become more well-rounded, foster a confrontational mindset, and develop their professional networks [9]. Institutional strength positively influences senior managers' perceptions of job security, default risks, financial risks, transaction costs, and regulatory control [10]. Internet deregulation is a new concept born out of the quick fame people can gain and the sense of comfort and confidence they gain from speaking freely online [11]. As hacking attacks on school and university data infrastructure become more common, students need to understand the impacts and issues of cyber security and cybercrime [12]. The most common way hackers use to gain unauthorized access to critical systems in a protected environment is through human factors. The web browser has become a very important tool for millions of students [13]. More and more students are using smartphones as learning tools. In comparison, cybersecurity issues related to the use of these devices in education appear to have received less attention [14]. The need for cyber security knowledge is now widely known, but the need for its wider application depends on the cyber security skills of employees [15]. It covers methods used to simulate phishing attacks, knowledge sharing, cybersecurity strategies, general phishing information, and cybersecurity awareness [16].

IMPORTANCE OF CYBERSECURITY FOR COLLEGE STUDENTS

College students often keep a large amount of personal information, from academic transcripts to financial data. Cybersecurity is essential to protect this sensitive information from loss and unauthorized access. Cybersecurity protects this intellectual property from theft or damage [3]. Cybersecurity is important to protect the confidentiality and integrity of online course materials and student information. Knowledge and experience in this field can open a variety of careers, including cybersecurity analyst, ethics analyst, and information security specialist. Security breaches can damage a student's reputation and jeopardize their career choices and educational aspirations [5]. Security issues can damage the university's reputation as shown in Figure 1.

Cybersecurity helps protect students from financial crimes, including identity theft and credit card fraud. Understanding cyber security is essential to complying with privacy laws and regulations. To comply with the law, it is important to know how to protect your data and report breaches. Learning about internet safety can help children develop good internet habits, including keeping passwords secure, updating computer systems, and avoiding phishing scams [7]. Cybersecurity expertise helps maintain relationships and communications.

© STM Journals 2024. All Rights Reserved

Figure 1. Importance of cybersecurity for college students.

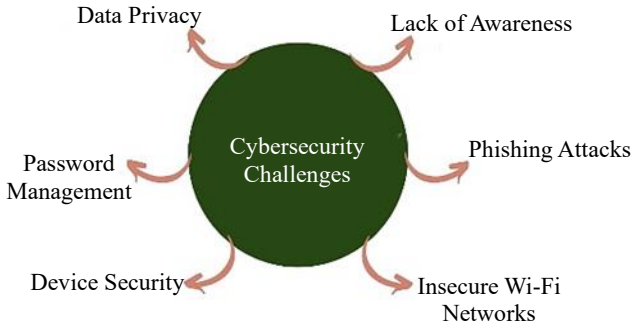

Figure 2. Cybersecurity challenges for college students.

Entrepreneurs want to protect their intellectual property and the technology they create. Cyber security is important to maintain the company's ideas and developments [14]. As responsible digital citizens, college students must understand the impact of their online behavior and how it affects not only themselves but society. Cybersecurity experience is helpful in this area. Safety awareness is a vital life skill, as is personal finance and communication.

CYBERSECURITY CHALLENGES FOR COLLEGE STUDENTS

Due to the widespread use of technology and online services, the online safety issues facing students are numerous and constantly evolving. Students often disclose personal information online and may be less careful about protecting their identity. Cybercriminals can steal personal data for financial gain or create credit cards or loans in students' names [9]. In response to these phishing attempts, students may inadvertently reveal sensitive information such as login passwords. Many students use weak or duplicate passwords on multiple accounts as shown in Figure 2.

Students may not fully understand the importance of online privacy settings on social media platforms. Excessive sharing or disclosure of personal data may lead to leakage of personal information and violation of privacy. While these networks are convenient, they can be unsecured, leaving students vulnerable to eavesdropping and man-in-the-middle attacks. Students may be encouraged to use digital technology to engage in unethical academic activities. Failure to update software, operating systems, and applications with security updates may expose students to vulnerabilities that could be exploited by fraudsters.

© STM Journals 2024. All Rights Reserved

Inadequate data backup methods can lead to data loss in the event of a ransomware attack or hardware failure. Students may miss important assignments, research papers, and assignments. Sharing files using unprotected techniques might lead to data breaches. Students routinely exchange documents with personal information, research data, and other sensitive stuff. Many students lack an understanding of cybersecurity best practices and may not know how to spot or respond to security risks effectively.

MAIN CYBER SECURITY CHALLENGES

Due to the increased use of technology and online services, college students face several online security challenges. There are several important challenges to cyber security, including:

Secure the Cloud

There is a concern that many companies are reluctant to store data in the cloud because they want to keep it before ensuring that the cloud is a highly secure location and complies with local security regulations. Large enterprise data centers are the main reason for this. Because the information is on their network and in their workplace, they have full control over it. In contrast, the cloud carries risks because the network is external, and the data is no longer stored in the company's data centers. Cloud misconfigurations, insecure APIs, Meltdown and Specter vulnerabilities, and data loss due to natural disasters or human error are among the causes of cloud attacks.

Attacks on Blockchain and Cryptocurrency Technologies

Technologies such as cryptocurrencies and blockchain have recently begun to gain popularity. Companies that adopt these technologies without implementing the necessary security controls present serious risks, as these technologies are still in their infancy and have a long way to go. In fact, companies may not even be aware of the vulnerabilities that exist. Therefore, it is recommended to research security measures before using these technologies. Eclipse and Sybil attacks are among the attacks launched.

Attacks Created Using Artificial intelligence (AI) and Machine Learning

There is no doubt that AI systems receive large amounts of data from around the world for various purposes, including helping people form opinions. While this is the positive side of things, there can also be a negative side. Hackers can develop innovative strategies that leverage AI and machine learning to launch more sophisticated attacks.

BEST PRACTICES FOR COLLEGE STUDENTS IN CYBER SECURITY

The adoption of effective online safety measures holds significant importance in mitigating the myriad challenges that students encounter within the digital realm. These methodologies can aid students in enhancing their virtual interactions and safeguarding their privacy.

It is recommended to generate complex and unique passwords for every online account to enhance security. Employ our password management tool to automatically generate, store, and input complex passwords. It is advised not to disclose personal identifying information, such as name, date of birth, or logo, for security and privacy reasons. It is advisable to implement multi-factor authentication (MFA) where applicable for securing online accounts. In order to mitigate the potential threat of unauthorized access to one's data, it is advisable to periodically modify one's password at intervals ranging from 3 to 6 months. Utilize privacy settings to regulate the dissemination of personal information on social networking platforms. It is advisable to exercise discretion in the disclosure of personal information to the public. It is advisable to refrain from accessing uncommon links or downloading files from unauthorized web sources. It is imperative to ensure that emails soliciting confidential or business-sensitive information are appropriate and adhere to established protocols. In order to mitigate vulnerabilities, it is essential to ensure that the operating system, software, and applications are regularly updated with the most recent security patches. It is important for individuals to develop the skill of identifying phishing attempts and to refrain from disclosing personal or financial information through email or text communications as shown in Figure 3.

© STM Journals 2024. All Rights Reserved

Figure 3. Best practices for college students in cyber security.

We recommend that you use a secure, private, and password-protected internet connection whenever possible, especially when you have sensitive business activities or access personal accounts online. We recommend that you use caution when connecting to public Wi-Fi networks and consider using a virtual private network for increased security. Sensitive information and documents must be protected against unauthorized access using encryption methods. When sending sensitive information, it is recommended that you use an encryption tool, or an encryption feature built into your communication program. Backing up your important files and documents can prevent data loss in the event of an attack or hardware failure. It is recommended to store backup copies of the data in a safe place or in the cloud service indicated in the source [15]. It is important to avoid using essays, cheats, or cheats when completing academic assignments. It is important to maintain intellectual integrity and ethical standards in academic work. It is important to establish a clear notification protocol for suspected cyber security breaches, data breaches, or identity theft. It is recommended that incidents be reported to campus security, IT Support, or the appropriate department. Gather the latest information on cybersecurity threats and effective mitigation strategies from popular articles, online resources such as blogs, and trusted sources.

CYBERSECURITY EDUCATION AND AWARENESS FOR COLLEGE STUDENTS

Security education and awareness play an important role in educating individuals, businesses, and communities about the information and skills needed to protect themselves in the digital age. Preventing security attacks: education and awareness programs can help individuals and organizations identify and mitigate cyber risks that can reduce the risk of a successful cyber-attack.

By understanding the importance of privacy and data protection, individuals can protect their personal information from theft or misuse. Training programs emphasize ethical behavior in online environments to avoid activities such as hacking, harassment, and fraud. Organizations that engage in cyber awareness and training can better protect their assets and maintain business continuity in the event of a cyber crisis [6]. National Security: In the context of a nation, cybersecurity training is essential to

© STM Journals 2024. All Rights Reserved

protect critical infrastructure, government networks, and sensitive data. Educate people about key digital skills, such as using the internet safely, identifying phishing scams, and practicing good password hygiene. Accredited cybersecurity courses offered by universities provide in-depth knowledge and skills to students seeking employment in the industry. We will continue to provide training and updates to keep people, staff, and students aware of new risks and restrictions. We organize interactive sessions, webinars, and hands-on training sessions to engage participants and reinforce cybersecurity topics as shown in Figure 4.

Create an accessible library of cybersecurity guides, white papers, and educational resources for anyone seeking knowledge. Conduct cyber security training and simulation exercises to assess business response capabilities and train employees on incident response. Government and non-government groups can launch public awareness campaigns to inform the public about cybersecurity threats and best practices. Align education and outreach activities with industry standards and best practices. Schools and parents should educate children about safe online activities from an early age, including the correct use of social media and gaming platforms. Organizations and educational institutions should design and implement cybersecurity policies and procedures to improve security culture [11]. Establish clear protocols for reporting cybersecurity issues to ensure rapid response and resolution. Encourage community participation in cybersecurity programs by creating a shared sense of responsibility and safety. Promote collaboration among academia, government, business, and the public to jointly solve network security issues.

CYBER SECURITY TECHNIQUES

Several cybersecurity measures protect individuals and businesses from online risks. The most common are a key cyber security measure is to use strong passwords for all accounts. This requires creating a unique password for each account, with a mix of upper- and lower-case letters, numbers, and special characters. To sign in with two-factor authentication, you need two forms of authentication. Such as mobile numbers and secure passwords. Firewalls restrict unauthorized information to the networks. They filter inside and outside messages that look like unused pieces of information. Antivirus software scans computers and the internet for viruses, malware, and other risks.

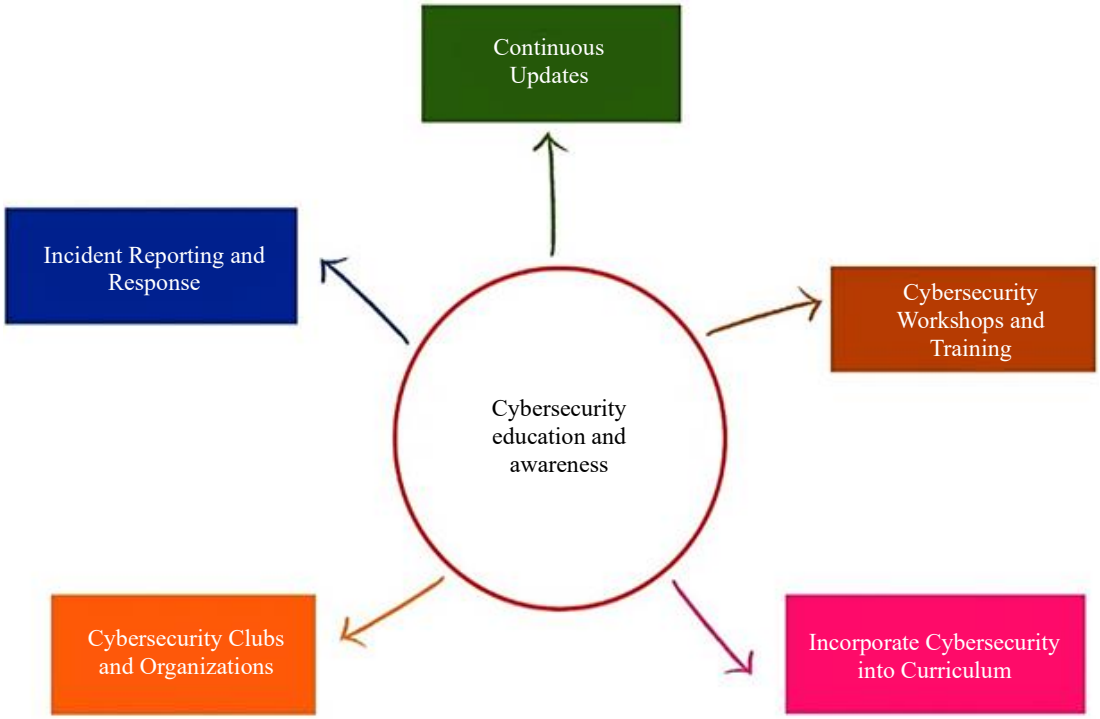

Figure 4. Cybersecurity education and awareness for college students.

© STM Journals 2024. All Rights Reserved

Security updates and bug fixes in software updates help prevent intrusions. For security reasons, update your software and operating system regularly. Encryption decodes data to prevent unwanted access to the information. This protects passwords, and financial and personal data [4]. Cybersecurity education is one of the most effective techniques. Phishing tactics, strong passwords, and monitoring and reporting of suspicious activity are all questionable. To protect against multiple threats, cybersecurity requires a multi-layered strategy that includes these and other measures.

CYBER SECURITY APPROACHES WITH SVM ALGORITHM

Machine learning allows robots to think like humans. Various machine learning algorithms allow computers to understand questions and try to find answers just like humans but in a very fast and accurate way. There are some types of machine learning algorithms are there. Supervised algorithms find answers to challenges with the help of humans. Unsupervised learning algorithms discover answers to questions without human interaction. The third path amplification algorithm is a combination of the two methods already described.

Support Vector Machine (SVM) is an excellent classification method for classification applications. The SVM method uses marginal values to perform the classification into two classes. Margins are determined using the distance between the closest profile features in each category. Hyperplanes are used to separate two classes of models very effectively. If the classification is based on more than two classes, multidimensional hyperplanes are used. Different parameters can be used as base values. Parameters can be polynomials. SVM technology can be used to identify IP addresses in the blacklist of other IP addresses.

Network Security uses the SVM algorithm to identify individuals with varying degrees of fraudulent intent. Secure Frame provides unique capabilities and methods to identify malicious URLs and IP addresses. However, the attacker used innovative methods to bypass their connections or requests to access the secure information stored on the server. Here, a Dshield dataset and a normalized dataset are created, which includes a list of malicious IP addresses and port addresses that contain malicious query strings. Here, the proposed system identifies and blocks malicious URLs (IPs) and port addresses. Protect apps and avoid evasion strategies.

DISCUSSION ON CYBERSECURITY FOR COLLEGE STUDENTS

Many real-life events and incidents have highlighted students' need for online safety. An important requirement for students is to prioritize digital security. When a student was using a public Wi-Fi network on campus, he fell victim to hackers who intercepted his online banking login information. Hackers continue to drain students' bank accounts. This incident highlights the need to protect personal information and the risks associated with unsecured networks. The university database stores male and female students. Personal information, including Social Security numbers and academic records, is disclosed. This hack will not only expose sensitive data but also lead to leakage of student data. identity, leading to potential financial fraud and reputational damage.

A student downloaded an article from a questionable website and submitted it as his work. The university's plagiarism detection program identifies sources that could have academic consequences. This case highlights the impact of unethical behavior and the need for academic integrity in the digital age. College students receive phishing emails that pretend to be official correspondence from a university's IT department. Some students fell for these scams and leaked their login information, leading to illegal access to their accounts and possible data leakage. Hackers attack the university IT infrastructure and encrypt important academic and administrative materials [8]. The agency had to pay a large ransom to access the encrypted material, demonstrating how devastating and costly ransomware attacks can be. Students are victims of online abuse and cyberbullying, where private photos and personal information are posted on social media without permission. This issue highlights the importance of online protection, cyber security awareness, and harassment reporting systems. Students

© STM Journals 2024. All Rights Reserved

often have limited financial resources and are vulnerable to online scams advertising scholarships, part-time jobs, or financial aid. Falling for these scams can lead to financial loss or even identity theft. Student work is being faked online, hurting their grades and academic progress.

This case highlights the importance of protecting academic data and the potential academic consequences of digital security breaches. These specific cases demonstrate that students are not immune to the cyber security threats that exist in the digital world. By understanding and prioritizing online safety, students can protect their personal information, academic standing, and financial well-being, and ultimately create a safer online environment for themselves.

FUTURE DIRECTIONS IN CYBERSECURITY FOR COLLEGE STUDENTS

Students' future path to cybersecurity depends on the expanding digital ecosystem and increasingly sophisticated cyberattacks. Preparing the next generation of professionals to deal with this challenging environment is crucial.

Here are some possible pointers for teaching and practicing cybersecurity to students. Educational institutions will offer interdisciplinary courses that combine cybersecurity with different research disciplines [5–7]. This approach will develop employees with specific expertise relevant to their career paths, such as healthcare cyber security, legal IT, and industrial control systems security. Cybersecurity education will go beyond the technical component to include digital literacy, train students to critically analyze information sources, practice online etiquette, and differentiate between trusted and untrusted digital content.

Practical training on ethical hacking and red teams will be introduced into cyber security programs. These activities will help students learn about and protect themselves from real-world risks and vulnerabilities as shown in Figure 5.

AI and machine learning (ML) in cybersecurity education will combine AI and machine learning methods to enable better threat detection, incident response, and security automation. Students will learn to use these techniques to improve their defenses. The course will focus on secure programming and application development methods, providing students with the skills needed to create programs and applications with built-in security features. Students will learn how to obtain, evaluate, and use threat intelligence data to proactively defend against emerging cyber threats.

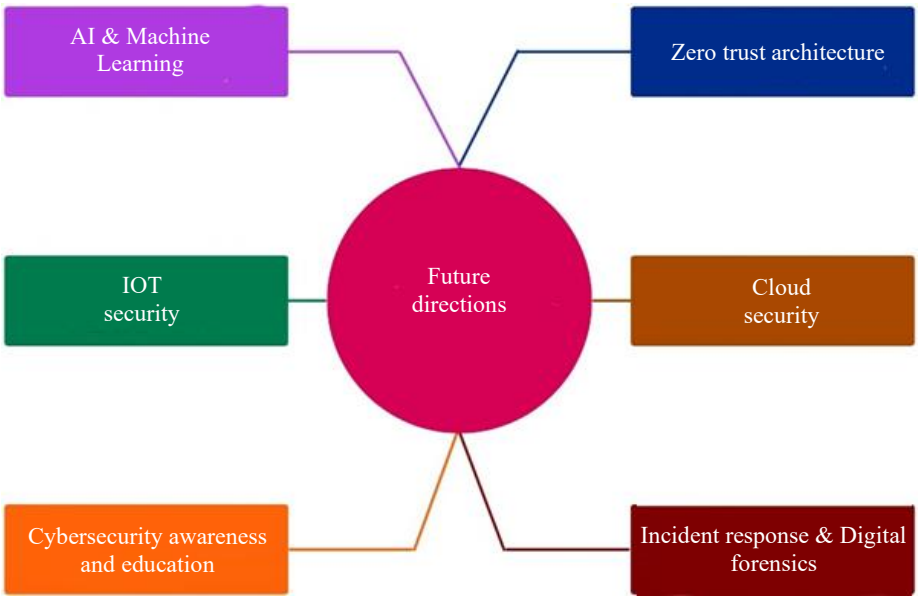

Figure 5. Future directions in cybersecurity for college students.

© STM Journals 2024. All Rights Reserved

Cyber Hygiene Education

Organizations will emphasize the need for appropriate cyber hygiene practices, including password management, software updates, and safe online behavior. Students will learn the legal and regulatory aspects of cybersecurity, preparing them for careers in compliance, risk management, and policy development. Cybersecurity education will focus on incident response and recovery strategies and train students to effectively manage and resolve security issues [13]. The course combines business, strategic, and cyber security knowledge to help students understand the wider impact of security on an organization and make informed decisions.

Agencies will create hands-on labs and replicate real-world scenarios to provide hands-on experience in combating cyber threats. As the cybersecurity landscape is rapidly evolving, organizations will work to create a culture of continuous learning and professional growth. Education will include a better public understanding of cybersecurity issues. Students will be encouraged to advocate for digital security and contribute to creating a secure digital society.

Encourage students to participate in network security competitions, hackathons, and capture-the-flag activities to improve their problem-solving skills and talents. Create mentoring programs to connect students with industry leaders and provide support and networking opportunities [15]. The future of cybersecurity education for university students will be characterized by adaptability and an understanding of the need for interdisciplinary knowledge, practical skills, and a strong ethical foundation. Preparing students to meet the challenges of a dynamic and ever-changing online ecosystem is critical to their future success and overall security in the connected world.

CONCLUSION

In the digital age, the safety of students online is crucial, as there are risks such as identity theft, privacy violations, phishing, and academic integrity issues. Students frequently encounter issues with weak passwords and engage in risky online behavior. Students' online lives are closely intertwined with academic research, social media, and personal finances, making them potential targets for cyberattacks. Protecting personal information is crucial because identity theft can lead to financial loss and bad credit. Protecting online privacy is crucial to preventing illegal access and cyberbullying.

Maintaining academic integrity is critical to ethical behavior and future employment opportunities. Improving digital skills and awareness of threats is crucial for children to navigate the digital world safely. Educational institutions should integrate cybersecurity training into their curricula to teach students how to properly manage passwords, phishing detection, and online privacy. Students should be made aware of the dangers of weak passwords and encouraged to use password managers and MFA. Academic institutions should establish clear cybersecurity policies and provide resources for incident reporting and support. Regular cyber security awareness programs, workshops, and hands-on training can help children protect their digital lives. Promoting ethical conduct online and stressing consequences for academic misconduct in the digital era.

Given the many risks facing the digital age, student safety online is paramount. To protect private information, online privacy, and academic integrity, it is important to recognize these issues and implement best practices. Educational institutions play a pivotal role in equipping students with the necessary knowledge and skills to navigate the digital realm securely.

REFERENCES

1. AlDaajeh S, Saleous H, Alrabaee S, Barka E, Breitinger F, Raymond Choo KK. The role of national cybersecurity strategies on the improvement of cybersecurity education. Comput Secur. 2022;119:102754. DOI: 10.1016/j.cose.2022.102754.
2. Chaudhary S, Gkioulos V, Katsikas S. A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Comput Sci Rev. 2023;50:100592. DOI: 10.1016/j.cosrev.2023.100592.

© STM Journals 2024. All Rights Reserved

3. Rohan R, Pal D, Hautamäki J, Funilkul S, Chutimaskul W, Thapliyal H. A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon. 2023;9. DOI: 10.1016/j.heliyon.2023.e14234.
4. Blažič BJ. The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. Technol Soc. 2021;67:101769. DOI: 10.1016/j.techsoc.2021.101769.
5. Cabaj K, Domingos D, Kotulski Z, Respício A. Cybersecurity education: Evolution of the discipline and analysis of master programs. Comput Secur. 2018;75:24–35. DOI: 10.1016/j.cose.2018.01.015.
6. Alanazi M, Freeman M, Tootell H. Exploring the factors that influence the cybersecurity behaviors of young adults. Comput Hum Behav. 2022;136:107376. DOI: 10.1016/j.chb.2022.107376.
7. Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J Comput Syst Sci. 2014;80:973–93. DOI: 10.1016/j.jcss.2014.02.005.
8. Smith CA, Masters PR. College students and patient work: Health information management by emerging young adults. Libr Inf Sci Res. 2023;45:101216. DOI: 10.1016/j.lisr.2022.101216.
9. Fisk N, Kelly NM, Liebrock L. Cybersecurity communities of practice: Strategies for creating gateways to participation. Comput Secur. 2023;132:103188. DOI: 10.1016/j.cose.2023.103188.
10. Ogbanufe O, Kim DJ, Jones MC. Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures. Inf Manage. 2021;58:103507. DOI: 10.1016/j.im.2021.103507.
11. Zorlu E. An examination of the relationship between college students' cyberbullying awareness and ability to ensure their personal cybersecurity. J Learn Teach Digit Age. 2023;8:55–70. DOI: 10.53850/joltida.1087377.
12. Alharbi T, Tassaddiq A. Assessment of cybersecurity awareness among students of Majmaah University. Big Data Cogn Comput. 2021;5:23. DOI: 10.3390/bdcc5020023.
13. Alqahtani MA. Factors affecting cybersecurity awareness among university students. Appl Sci. 2022;12:2589. DOI: 10.3390/app12052589.
14. Taha N, Dahabiyeh L. College students information security awareness: A comparison between smartphones and computers. Educ Inf Technol. 2021;26:1721–36. DOI: 10.1007/s10639-020-10330-0.
15. Blažič BJ. Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? Educ Inf Technol. 2022;27:3011–36. DOI: 10.1007/s10639-021-10704-y.
16. Daengsi T, Pornpongtechavanich P, Wuttidittachotti P. Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Educ Inf Technol. 2022;27:4729–52. DOI: 10.1007/s10639-021-10806-7.

© STM Journals 2024. All Rights Reserved