Computer Education Research Journal (CERJ)
Volume 10 Issue No: 1 pp. 98-110 (2024) Website: https://www.cerj.com.ng

Published Online: 15th July, 2024

Skill Needs of Computer Education Students in Preventing Cyber Insecurity and Unethical Hacking in the University of Nigeria Nsukka

Fadip Audu Nannim[1], Maryrose Oluchi Eze[1], Bridget Ijeoma Eneh[2], Chukwuma Juliet Ogochukwu[2], Asogwa Blessing Ebere[2], Ugwuoka Chinwe[2]

[1]Department of Computer and Robotics Education, University of Nigeria, Nsukka
[2]Department of Computer Science, Enugu State College of Education Technical, Enugu
Corresponding Author: fadip.nannim@unn.edu.ng

Abstract

This study sought to determine the skill needs of computer education students in preventing cyber insecurity and unethical hacking at the University of Nigeria Nsukka. The study adopted a descriptive survey research design approach and the population for the study is 116 students of Computer and Robotics Education. A total sampling technique was used to select all the Computer and Robotics Education Students in the University of Nigeria Nsukka as sample for the study. The instrument used for data collection was a structured questionnaire titled: "Skill Needs of Computer Education Students in Cyber Insecurity and Unethical Hacking Questionnaire" (SNCIUHQ). Three experts validated the instrument and have an overall reliability index of .94. Mean and standard deviation were statistics used for data analysis. The result of this study identified four major skills needed for combating cyber insecurity and unethical hacking to include networking and system administration skills, knowledge of operating systems and virtual machines, networking security controls and coding skills. The strategies for the effective prevention of cyber insecurity and unethical hacking were also identified. It was recommended that the university should consider revising and updating its computer education curriculum to include specialized courses and modules focused on cybersecurity and ethical hacking among others.

Keyword: Cyber Insecurity; Unethical Hacking; University; prevention, computing students

Introduction

The historical background of ethical hacking and cybersecurity dates back several decades and has evolved alongside the growth of computer technology and the rise of the internet (Arum, 2021). In the early days, hacking was more of an exploratory activity. Many hackers focused on learning and sharing knowledge rather than causing harm. In the 1980s, as computer systems became more prevalent in businesses and governments, security concerns emerged. The first notable cyber incidents, such as the Morris Worm in 1988, raised awareness about the need for protection against malicious attacks (Ngo et al., 2020).

As hacking activities started to become more malicious, a distinction emerged between "hackers" (those with a passion for exploration) and "crackers" (those who engaged in hacking with malicious intent). This differentiation helped set the stage for ethical hacking, emphasizing the positive use of hacking skills. Hacker groups like The Legion of Doom and The Chaos Computer Club gained prominence during this period (Ulrich et al., 2023). These communities acted as platforms for knowledge exchange but also drew attention from law enforcement agencies

due to some members engaging in illegal activities. In the early 1990s, a series of high-profile cybercrimes, such as the hacking of major corporations and government systems, led to increased public concern. This resulted in law enforcement agencies cracking down on hacking activities, leading to the arrest and prosecution of several hackers.

Prevention of unethical hacking and cyber insecurity in Nigeria has become a pressing concern, prompting the implementation of comprehensive computer education programs in tertiary institutions. Recognizing the need to equip students with the knowledge and skills to combat cyber threats, these studies focus on fostering a strong understanding of cybersecurity principles, ethical hacking practices, and risk management strategies. This concerted effort aims to produce a new generation of cybersecurity professionals capable of safeguarding Nigeria's digital infrastructure (Odumesi, 2014). As the need for proactive cybersecurity measures became evident, organizations began realizing the value of harnessing the skills of hackers for defensive purposes.

The term "ethical hacking" gained popularity, referring to authorized security assessments performed by skilled individuals to identify vulnerabilities (Yaacoub et al., 2021). In response to the growing demands for ethical hacking, laws and policy frameworks were established to legitimize the practice, such as penetrating systems and networks with intention of identifying and resolving vulnerabilities. Organizations recognized the importance of conducting regular security assessments and started hiring cybersecurity professionals to help protect their systems. The field of cybersecurity has grown rapidly, driven by technological advancements and an ever-evolving threat landscape. New tools, techniques, and methodologies have been developed to safeguard digital systems and networks from cyberattacks. With the increasing interconnectedness of the world, cyber threats have become a global concern (Fjäder, 2016). Cybersecurity has gained prominence on the international stage, with governments, organizations, and individuals recognizing the need for robust security measures to protect critical infrastructure and sensitive data (Lewis, 2019).

Cyber insecurity refers to the state of vulnerability and risk in the digital realm, where computer systems, networks, and data are susceptible to unauthorized access, exploitation, or malicious activities. It encompasses the lack of proper security measures, practices, and defences that can lead to cyber-attacks, data breaches, and other forms of cybercrime (Alzubaidi, 2021). It can result from various factors, including technological vulnerabilities, human errors, inadequate security protocols, and evolving cyber threats.

Nigeria has witnessed rapid growth in its digital landscape over the past decade. With a large population and increasing internet penetration, the country has become a fertile ground for cyber activities. Unfortunately, this growth has also resulted in an upsurge of cybercrimes, including unethical hacking, data breaches, and phishing attacks (Ayub & Linus, 2022). These threats have severe consequences for individuals, businesses, and the overall development of the nation. Unethical hacking and cyber insecurity have multifaceted impact on Nigeria's society and economy. Financial losses resulting from data breaches and fraud affect both individuals and organizations, hindering economic growth. Additionally, compromised privacy can lead to identity theft, blackmail, and reputational damage. National security is also at risk, as cyber-attacks can disrupt critical infrastructure, compromise government systems, and facilitate espionage or terrorism. Given these consequences, addressing unethical hacking and cyber insecurity is crucial for Nigeria's overall well-being. Tertiary

institutions in Nigeria, including universities and polytechnics, have a unique opportunity to address the challenges of unethical hacking and cyber insecurity. By offering computer education programs, these institutions can equip students with the necessary knowledge and skills to understand, prevent, and respond to cyber threats effectively (Crumpler & Lewis, 2019).

The Nigerian government has recognized the seriousness of these threats and has taken several measures to address them. The Cybercrime Act of 2015, for example, criminalizes cybercrime and provides for punishment for offenders. Also, the National Information Technology Development Agency (NITDA) has developed a national cybersecurity policy and strategy to guide cybersecurity efforts in the country. However, these measures alone are not enough to eradicate unethical hacking and cyber insecurity as the rate of cybercrime appears to be on the increase within the country (Afolabi, 2023). There is therefore a need for a more comprehensive approach that involves promoting computer education in tertiary institutions. These approaches recognize that the lack of knowledge and skills among computer users is a major factor in the vulnerability of computer systems to cyber threats.

Furthermore, Nigeria like many other countries around the world, has been facing the challenge of unethical hacking and cyber insecurity for several years (Yusuf, 2014). With the rapid advancements in technology and the widespread use of the internet, criminals have found new avenues to exploit vulnerabilities in computer systems and networks. Cyberattacks have grown increasingly sophisticated and devastating resulting in substantial financial losses for businesses and individuals, while also endangering sensitive information (Afolabi, 2023). Considering this, the traditional computer education programme in Nigeria which focused primarily on basic computer literacy and programming skills should now be refocused to recognizing that cybersecurity should be an integral component of tertiary-level computer education programmes.

Consequently, students should not only be instructed on computer usage but also be trained in safeguarding computers against cyber threats. To achieve this objective, there is a need to develop comprehensive computer education programs encompassing various topics related to cybersecurity. These programs should include courses on network security, cryptography, ethical hacking, and cybercrime investigation. Additionally, students should be educated on the legal and ethical dimensions of cybersecurity, as well as acquiring cyber insecurity and unethical hacking prevention skills. Some of these cybersecurity and ethical skills according to Jena (2024) include network and system administration skills (in-depth understanding of networking, configuring and maintaining computers), knowledge of operating systems and virtual machines (strong knowledge of operating environments such as Windows, Linux, and Mac OS), network security control (different measures which are employed to enhance the security of a network), coding skills (ability to explicitly instruct the computer using languages such as C, C++, Python, JavaScript, Java, SQL, HTML etcetera) among others.

Therefore, the main purpose of this study is to investigate the skill needs of computer education students in preventing cyber insecurity and unethical hacking at the University of Nigeria Nsukka.

Research Questions

The following research questions were raised to guide the study:

1. What are the networking and system administration skills for preventing cyber insecurity and unethical hacking among computer education students?
2. What is the knowledge of operating systems and virtual machines

required for preventing cyber insecurity and unethical hacking among computer education students?

3. What are the networking security controls for required for preventing cyber insecurity and unethical hacking among computer education students?
4. What are the coding skills needed required for prevent cyber insecurity and unethical hacking among computer education students?
5. What are the strategies for the effective prevention of cyber insecurity and unethical hacking?

Methodology

This study adopted the descriptive survey research design. The descriptive survey research design focuses on people, their vital facts, beliefs, opinions, attitudes, motivation and behaviour as well as situations currently obtained (De Vaus, & de Vaus, 2013), hence appropriate for this study. The population for this study is 116 students of Computer and Robotics Education at the University of Nigeria Nsukka, comprising 70 female and 46 male students. This encompasses students across different academic years and semesters. Because of this small population size, the total sampling technique was used. Hence, a total of 116 students participated in the study. The instrument used for data collection was a 41-item structured questionnaire titled: "Skill Needs of Computer Education Students in Cyber Insecurity and Unethical Hacking Questionnaire" (SNCIUHQ). The questionnaire was grouped into five clusters on a 4-point rating scale of Strongly Agreed (SA), Agreed (A) Disagreed (D), and Strongly Disagreed (SD) with assigned weights of 4, 3, 2 and 1 respectively. The instrument was validated by three experts from the Computer and Robotics Education, University of Nigeria Nsukka. The reliability of the instrument tested using Cronbach's Alpha yielded the following reliability indexes: 0.71, 0.772, 0.81, 0.90, and 0.89 for Cluster A, B, C, D, and E respectively. The instrument has an overall reliability index of 0.95. This means that the instrument has a very high reliability and internal consistency to measure what it is supposed to measure. The researcher collected the data with the help of four research assistants. The data collected was analysed using mean and standard deviation. For decision-making, a criterion mean of 2.5 and above was considered as an "Agreed", while, items below 2.5 mean ratings were considered as "Disagreed".

Results

The results of this study were presented based on the research questions guiding the study.

Research Question One

What are the networking and system administration skills for preventing cyber insecurity and unethical hacking among computer education students?

Table 1: Mean and Standard Deviation on Networking and System Administration Skills for Preventing Cyber Insecurity and Unethical Hacking among Computer Education students

S/N	Item Statements	N	$\bar{x}$	SD	Decision
1	Networking skills is required by system administration for prevention of cyber insecurity and unethical hacking	114	3.54	0.63	Agreed
2	Knowledge of data transmission techniques is important in securing data	114	3.47	0.58	Agreed
3	Having system administration skills will be beneficial for you in the prevention of cyber insecurity and unethical hacking	114	3.34	0.69	Agreed
4	Ability to use various features and settings of the computer system is very important"	114	3.49	0.63	Agreed
5	Ability to use regular software updates and patching skill	114	3.39	0.76	Agreed
6	Ability to use network configuration setup skill	114	3.35	0.64	Agreed
7	Ability to use backup and disaster recovery skills	114	3.54	0.55	Agreed
	Cluster mean	**114**	**3.45**	**0.39**	**Agreed**

Key: N = Number of respondents; $\bar{x}$ = Mean; SD = Standard Deviation; $\bar{x} \geq 2.50 = Agreed, < 2.50 = Disagreed$

Results in Table 1 show that the respondents agreed to all the items as networking and system administration skills required for preventing cyber insecurity and unethical hacking among computer education students. These items had their mean ratings above the criterion mean of 2.5, hence, all the items were agreed to. The cluster mean of 3.45±0.39 shows that overall, the respondents strongly agreed to all the items as networking and system administration skills required for preventing cyber insecurity and unethical hacking among computer education students. A standard deviation of 0.39 shows that on average, the respondents do not differ much in their responses.

Research Question 2

What is the knowledge of operating systems and virtual machines for preventing cyber insecurity and unethical hacking among computer education students?

Table 2: Mean and Standard Deviation on knowledge of operating systems and virtual machines for preventing cyber insecurity and unethical hacking among computer education students

S/N	Item Statement	N	$\bar{x}$	SD	Decision
8	Cybersecurity professional must have a strong knowledge of operating environments such as Windows, Linux, and Mac OS	114	3.54	0.64	Agreed
9	Cybersecurity experts should be familiar with the security features provided by modern operating systems	114	3.57	0.60	Agreed
10	Cybersecurity experts should be comfortable working on any OS	114	3.43	0.52	Agreed
11	Ability to install and configure an operating system on a virtual machine is important in prevention of cyber insecurity and unethical hacking	113	3.52	0.55	Agreed
12	Cybersecurity professional be able to differentiate between a host operating system and a guest operating system in a virtualization environment	114	3.43	0.64	Agreed
13	Ability to troubleshoot common issues that may arise when running virtual machines	114	3.38	0.78	Agreed
14	Understanding operating systems and virtual machines is essential for overall computer security	114	3.56	0.50	Agreed
	Cluster Mean	**114**	**3.49**	**0.40**	**Agreed**

Key: N = Number of respondents; $\bar{x}$ = Mean; SD = Standard Deviation; $\bar{x} \geq 2.50 = Agreed, < 2.50 = Disagreed$

Results in Table 2 show that the respondents agreed that these 7 items are knowledge of operating systems and virtual machines for preventing cyber insecurity and unethical hacking among computer education students. These items had their mean ratings above the criterion mean of 2.5, hence, all the 7 items were accepted. The cluster mean of 3.49±0.40 shows that overall, the respondents strongly agreed that these 7 items are knowledge of operating systems and virtual machines is important for preventing cyber insecurity and unethical hacking among computer education students. A standard deviation of 0.40 shows that on average, the respondents do not differ much in their responses.

Research Question 3

What are the networking security controls for preventing cyber insecurity and unethical hacking among computer education students?

Table 3: Mean and Standard Deviation on Networking Security Controls for Preventing Cyber Insecurity and Unethical Hacking among Computer Education Students

S/N	Item Statements	N	$\bar{x}$	SD	Decision
15	Ability to know how your network works	114	3.62	0.59	Agreed
16	Knowledge of firewall to filter and prevent unauthorized traffic into the network	114	3.55	0.60	Agreed
17	Ability to know how the router works and be able to use it effectively	114	3.54	0.58	Agreed
18	Ability to know the purpose of intrusion detection systems and intrusion prevention systems in network security	114	3.46	0.64	Agreed
19	ability to differentiate between network-based and host-based intrusion detection system	114	3.58	0.60	Agreed
20	Knowledge of Intrusion detection system (IDS) and ability to recognize any security policy violations and malicious traffic on the network	114	3.52	0.55	Agreed
21	Ability to use network monitoring tools such Wireshark in identifying suspicious activities	114	3.53	0.61	Agreed
22	Ability to know that implementing strong network security controls is essential in preventing cyber threats	114	3.46	0.68	Agreed
	Cluster3 Mean	**114**	**3.53**	**0.40**	**Agreed**

Key: N = Number of respondents; $\bar{x}$ = Mean; SD = Standard Deviation; $\bar{x} \geq 2.50 = Agreed, < 2.50 = Disagreed$

Results in Table 3 show that the respondents agreed that these 8 items are networking security controls for preventing cyber insecurity and unethical hacking among computer education students. These items had their mean ratings above the criterion mean of 2.5, hence, all the 8 items were agreed to. The cluster mean of 3.53±0.40 shows that overall; the respondents strongly agreed that these 8 items are networking security controls for preventing cyber insecurity and unethical hacking among computer education students. The standard deviation of 0.40 shows that on average, the respondents do not differ much in their responses.

Research Question Four

What are the coding skills needed to prevent cyber insecurity and unethical hacking among computer education students?

Table 4: Mean and Standard Deviation on Coding Skills Needed to Prevent Cyber Insecurity and Unethical Hacking among Computer Education Students

S/N	Items Statements	N	$\bar{x}$	SD	Decision
23	Having zero coding knowledge may limit your cybersecurity opportunities in the future	114	3.68	0.52	Agreed
24	Ability to use C	114	3.55	0.60	Agreed
25	Ability to use C++	114	3.51	0.68	Agreed
26	Ability to use Python	114	3.54	0.58	Agreed
27	Ability to use JavaScript	112	3.55	0.64	Agreed
28	Ability to use PHP	114	3.57	0.65	Agreed
29	Ability to use HTML	114	3.45	0.83	Agreed
30	Ability to use Go lang	114	3.41	0.80	Agreed
31	Ability to use SQL	113	3.48	0.61	Agreed
32	Ability to use Assembly Language	114	3.57	0.53	Agreed
	Cluster4 Mean	**114**	**3.521**	**0.47**	**Agreed**

Key: N = Number of respondents; $\bar{x}$ = Mean; SD = Standard Deviation; $\bar{x} \geq 2.50 = Agreed, < 2.50 = Disagreed$

Results in Table 4 show that the respondents agreed that these 10 items are coding skills needed to prevent cyber insecurity and unethical hacking among computer education students. These items had their mean ratings above the criterion mean of 2.5, hence, all 10 items were accepted. The cluster mean of 3.52±0.47 shows that overall; the respondents strongly agreed that these 10 items are coding skills needed to prevent cyber insecurity and unethical hacking among computer education students. A standard deviation of 0.47 shows that on average, the respondents do not differ much in their responses.

Research Question Five

What are the strategies for the effective prevention of cyber insecurity and unethical hacking?

Table 5: Mean and Standard Deviation on Strategies for the Effective Prevention of Cyber Insecurity and Unethical Hacking

S/N	Item Statements	N	$\bar{x}$	SD	Decision
33	Comprehensive cybersecurity education and training are crucial in combating cyber insecurity and unethical hacking	114	3.65	0.58	Agreed
34	Raising user awareness about cybersecurity risks and best practices is effective in mitigating cyber threats	114	3.66	0.53	Agreed
35	Regular software updates and patch management are effective in preventing cyber vulnerabilities and exploits	114	3.66	0.55	Agreed
36	Advanced network security controls such as firewalls, intrusion detection play a significant role in safeguarding against cyberattacks	114	3.52	0.80	Agreed
37	Encryption and data protection mechanisms are effective in securing sensitive information from unauthorized access	114	3.54	0.68	Agreed
38	Sharing threat intelligence and cybersecurity information among organizations is extremely important in enhancing overall security	113	3.52	0.66	Agreed
39	Having a well-defined incident response plan is very valuable in minimizing the impact of cyber incidents and breaches	113	3.57	0.64	Agreed
40	Legal and regulatory measures are very effective in deterring cybercriminals and unethical hackers	114	3.48	0.61	Agreed
41	Ethical hacking (authorized penetration testing) is very beneficial in identifying and addressing vulnerabilities.	114	3.58	0.61	Agreed
	Clsuter Mean	**114**	**3.57**	**0.47**	**Agreed**

Key: N = Number of respondents; $\bar{x}$ = Mean; SD = Standard Deviation; $\bar{x} \geq 2.50 = Agreed, < 2.50 = Disagreed$

The results in Table 5 show that the respondents agreed to all the 9 items as strategies for the effective prevention of cyber insecurity and unethical hacking. These items had their mean ratings above the criterion mean of 2.5, hence, all the 9 items were accepted. The cluster mean of 3.57±0.47 shows that overall, the respondents strongly agreed to all the 9 items as strategies for the effective prevention of cyber insecurity and unethical hacking. A standard deviation of 0.47 shows that on average, the respondents do not differ much in their responses.

Discussion of Findings

This section discussed the result of the study based on research questions guiding the study. Results from research question one showed the networking and system administration skills for preventing cyber insecurity and unethical hacking required computer education students. Findings from this research question showed that the all the skills listed such as Ability to use various features and settings of the computer system, Ability to use regular software updates and patching skill, Ability to use network configuration setup skill, Ability to use backup and disaster recovery skills, Knowledge of data transmission techniques is important in securing data were all required skills. The cluster mean shows that these skills were strongly agreed as networking and system administration skills required for preventing cyber insecurity and unethical hacking among computer education students. This result agrees with Singh and Lien (2023); Ibrahim et al. (2020) who emphasized the importance of networking and system administration skills in preventing cyber insecurity and unethical hacking.

Results from research question two identified the knowledge of operating systems and virtual machines for preventing cyber insecurity and unethical hacking among computer education students. Finding from this research question showed the various skills needed which includes : knowledge of operating environments such as Windows, Linux, and Mac OS, being familiar with the security features provided by modern operating systems, ability to install and configure an operating system on a virtual machine, ability to differentiate between a host operating system and a guest operating system in a virtualization environment, ability to troubleshoot common issues that may arise when running virtual machines, understanding operating systems and virtual machines is essential for overall computer security. The cluster mean shows that these skills were strongly agreed as knowledge of operating systems and

virtual machines for preventing cyber insecurity and unethical hacking among computer education students. This result agrees with previous studies which showed that virtual machines are an effective tool for teaching security concepts, as they allow students to safely experiment with different types of software and operating systems (Yamin et al., 2021; Hernandez-de-Menendez et al., 2020).

Results from research question three showed that Ability to know how your network works, knowledge of firewall to filter and prevent unauthorized traffic into the network, ability to know how the router works and be able to use it effectively, ability to know the purpose of intrusion detection systems and intrusion prevention systems in network security, ability to differentiate between network-based and host-based intrusion detection system, knowledge of Intrusion detection system (IDS) and ability to recognize any security policy violations and malicious traffic on the network, ability to use network monitoring tools such Wireshark in identifying suspicious activities, ability to use network monitoring tools such Wireshark in identifying suspicious activities are the networking security controls for preventing cyber insecurity and unethical hacking among computer education students. This result agrees with Asghar et al. (2019) who showed that possessing network security control skills is an effective strategy for cybersecurity and prevention of unethical hacking.

Results from research question four showed that the ability to use programming languages like C, ability to use C++, ability to use Python, ability to use JavaScript, ability to use PHP, ability to use HTML, ability to use Go lang, ability to use SQL, ability to use Assembly Language are coding skills needed to prevent cyber insecurity and unethical hacking among computer education students. This result agrees with Ghelani (2018) who stated that computer programming can be used to develop computational thinking skills, which are important for cybersecurity.

The study identified strategies for the effective prevention of cyber insecurity and unethical hacking to include: comprehensive cybersecurity education and training are crucial in combating cyber insecurity and unethical hacking. Raising user awareness about cybersecurity risks and best practices is effective in mitigating cyber threats, regular software updates and patch management are effective in preventing cyber vulnerabilities and exploits. Advanced network security controls such as firewalls, intrusion detection play a significant role in safeguarding against cyberattacks, encryption and data protection mechanisms are effective in securing sensitive information from unauthorized access. Also, sharing threat intelligence and cybersecurity information among organizations is extremely important in enhancing overall security, having a well-defined incident response plan is very valuable in minimizing the impact of cyber incidents and breaches, legal and regulatory measures are very effective in deterring cybercriminals and unethical hackers, ethical hacking (authorized penetration testing) is very beneficial in identifying and addressing vulnerabilities. These results agreed with many authors e.g. (Masenya, 2023; Renaud et al., 2021) who identified similar strategies as effective ways of preventing cyber insecurity and unethical hacking

Conclusion

This study was conducted to determine the skill needs of computer education students in preventing cyber insecurity and unethical hacking in university of Nigeria Nsukka. This became necessary to reverse the present high rate of unethical hacking and cyber insecurity which affect basically all aspects

of modern life and it is coevolving with the progress of technology. Many individuals and organizations remain unaware of the potential risks and consequences of cybersecurity. Many individuals fall victim to phishing scams or using weak passwords. These may result in financial losses, data breaches, disruption of services, intellectual property theft, and national security concerns. However, if unethical hacking could be mitigated, the absence of unethical hacking would indicate that digital assets, including personal information, financial systems, and critical infrastructure, are adequately protected. Therefore, it is imperative that educational institutions adapt their curricula to equip students with the knowledge and skills necessary to navigate the complex and ever-changing world of cyber insecurity and unethical hacking. The findings of this study provide valuable insights for educators, policymakers, and stakeholders to better prepare the next generation of computer professionals to safeguard our digital future and uphold ethical standards in the field of cybersecurity.

Recommendations

Based on the findings and conclusions drawn from the study, the following recommendations were made that:

1. The university should consider revising and updating its computer education curriculum to include specialized courses and modules on networking, and coding focused on cybersecurity and ethical hacking.
2. Provide training and development opportunities for faculty members to ensure they are up-to-date with the latest trends and technologies in cybersecurity. This will enable them to effectively teach and mentor students in this field.
3. Emphasize the importance of ethical behaviour and responsible hacking practices throughout the curriculum.
4. Invest in well-equipped cybersecurity laboratories where students can gain hands-on experience in a controlled environment, experimenting with security tools and techniques.
5. Encourage students to engage in cybersecurity research projects fostering innovation and contributing to the field's knowledge base.

References

Afolabi, B. (2023, April, 28). NITDA urges countries to develop global cyber policies. Punch Newspaper. https://punchng.com/nitda-urges-countries-to-develop-global-cyber-policies/

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1). https://doi.org/10.1016/j.heliyon.2021.e06016

Arum, B. U. (2021). Hacking and cyber security in Nigeria telecommunication industry: Implication for teaching and learning. *SIST Journal of Religion and Humanities*, *1*(1).

Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946. https://doi.org/10.1016/j.comnet.2019.106946

Ayub, A. O., & Linus, A. (2022). Trends, Patterns and Consequences of Cybercrime in Nigeria. *Gusau International Journal of Management and Social Sciences*, *5*(1), 22-22.

https://gijmss.com.ng/index.php/gijmss/article/view/107

Crumpler, W., & Lewis, J. A. (2019). *The cybersecurity workforce gap* (p. 10). Washington, DC, USA: Center for Strategic and International Studies (CSIS).

De Vaus, D., & de Vaus, D. (2013). *Surveys in social research*. Routledge.

Fjäder, C. O. (2016). National security in a hyper-connected world: Global interdependence and national security. *Exploring the security landscape: Non-traditional security challenges*, 31-58. https://doi.org/10.1007/978-3-319-27914-5_3

Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*. https://doi.org/10.22541/au.166385206.63311335/v1

Hernandez-de-Menendez, M., Escobar Díaz, C. A., & Morales-Menendez, R. (2020). Educational experiences with Generation Z. *International Journal on Interactive Design and Manufacturing (IJIDeM)*, *14*, 847-859. https://doi.org/10.1007/s12008-020-00674-9

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020, June). A study on cybersecurity challenges in e-learning and database management system. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-5). IEEE. https://ieeexplore.ieee.org/abstract/document/9116415

Jena, B. K. (2024). *Top 8 cybersecurity skills you must have*. https://www.simplilearn.com/tutorials/cyber-security-tutorial/cyber-security-skills

Lewis, T. G. (2019). *Critical infrastructure protection in homeland security: defending a networked nation*. John Wiley & Sons.

Masenya, T. M. (2023). Awareness and knowledge of cyber ethical behaviour by students in higher education institutions in South Africa. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 33-48). IGI Global. https://doi.org/10.4018/978-1-6684-7207-1.ch002

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious software threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793-813.

Odumesi, J. O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116-125.

Renaud, K., Searle, R., & Dupuis, M. (2021, October). Shame in cyber security: effective behavior modification tool or counterproductive foil?. In *New Security Paradigms Workshop* (pp. 70-87). https://doi.org/10.1145/3498891.3498896

Singh, N., & Lien, L. (2023). *Ethical Hacking as a Risk Management tool in Organizations* (Master's thesis, Nord universitet).

Ulrich, F., Müller, S. D., & Flowers, S. (2023). The Professionalization of Hackers: A Content Analysis of 30 Years of Hacker Communication. *Communications of the Association for Information Systems*, *52*(1), 12. https://doi.org/10.17705/1CAIS.05246

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A survey on ethical hacking: issues and challenges. *arXiv preprint arXiv:2103.15072*. https://doi.org/10.48550/arXiv.2103.15072

Yamin, M. M., Katt, B., & Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security*, *110*, 102450. https://doi.org/10.1016/j.cose.2021.102450

Yusuf, I. B. (2014). Cyber threats and national security in Nigeria: challenges and options. *NDC E-Journal*, *13*(2), 131-146. https://ndcjournal.ndc.gov.bd/ndcj/index.php/ndcj/article/view/133

