ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

Exploring Strategies in Teaching Cybersecurity Measures Among Criminology Students

Meryll Anne M. Rulida[1]; Henna Marie M. Abad[2]; Allya Claire S. Auxtero[3]; Irish P. Bandolos[4]

[4]PhD

[1,2,3,4]University of Mindanao

Publication Date: 2026/10/31

Abstract: This study explored the teaching strategies, learning experiences, challenges, and real-world applications of cybersecurity education among criminology students. Using a qualitative research design, data were collected through in-depth interviews to capture students' perspectives on how cybersecurity concepts are taught and applied. The findings revealed that instructors primarily use lecture-based instruction supported by multimedia tools, along with application-driven and collaborative learning strategies. Students demonstrated better understanding when theoretical concepts were connected to real-life scenarios, case analysis, and experiential activities; however, challenges such as the complexity of cybercrime laws and technical concepts, as well as limited access to digital resources, laboratory tools, and hands-on learning opportunities, were also identified. Despite these limitations, students were able to apply cybersecurity knowledge in real-world and simulated contexts, particularly in digital investigation, personal data protection, and cyber threat awareness. The study concludes that effective cybersecurity education requires a balanced integration of theory and practice, supported by adequate technological resources and experiential learning opportunities to better prepare students for real-world cybersecurity challenges.

Keywords: *Teaching Strategies, Cybercrime, Experiential Learning, Digital Security, Hands-on Learning, Case Analysis, Criminology Students, Simulation-Based Learning.*

SDG Indicator: *#4 Quality Education #16 Peace, Justice, and Strong Institutions.*

How to Cite: Meryll Anne M. Rulida; Henna Marie M. Abad; Allya Claire S. Auxtero; Irish P. Bandolos (2026) Exploring Strategies in Teaching Cybersecurity Measures Among Criminology Students. *International Journal of Innovative Science and Research Technology*, 11(9), 3478-3492. https://doi.org/10.38124/ijisrt/26sep056

I. INTRODUCTION

In today's digital world, cyber threats are becoming a bigger concern, particularly among university students who use the internet for both their social and academic lives. Many students have accounts compromised and then used to spread malicious links on social media platforms such as Facebook. Many of these incidents are linked to phishing attacks, in which users are tricked into disclosing their login credentials (Alabab et al., 2023). Schools are also seen as vulnerable to cyber threats because many online attacks target academic environments, often through unattended or compromised accounts.

Cybersecurity has become an important issue in schools because many cyberattacks begin when the online predator gains access to a person's account. About three out of every four cyberattacks involve compromised accounts, putting both students and educational institutions at risk, according to Netwrix (2023). Students may struggle to achieve the expected learning outcomes if they are not given sufficient opportunities to practice their cybersecurity skills. According to Churi and Rao (2021), students' cybersecurity skills may not be fully assessed when instruction relies mainly on lectures and oral recitations.

As cybercrime increases, criminology students need to learn not only the concepts but also how to apply them in real-world situations. However, understanding Cybersecurity does not always mean people will apply what they know. A study by Concoles et al. (2022) found that criminology students at Central Mindanao Colleges generally exhibit high levels of cybersecurity awareness and a preventive attitude, suggesting that they are already aware of cybersecurity issues and understand the importance of protecting themselves online. Institutions should focus on teaching strategies that may help students apply their knowledge.

The importance of this study lies in its ability to improve cybersecurity instruction tailored for criminology

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

students. Educational institutions and organizations place a high priority on Cybersecurity as an integral part of their information and communication technology, given the evolving threat landscape (Hobbs, 2023). So, integrating practical applications or simulations into cybersecurity teaching will not only improve students' ability to identify fraudulent emails and other forms of attack but also enhance their capacity to address real-life scenarios. Preventing the occurrence of cyber victimization by their relatives or peers. Moreover, this study aims to reduce victimization and enable criminology students to become proactive defenders against cybercrime by offering an evidence-based framework for creating targeted online crime prevention education that can be utilized by teaching personnel (Concoles et al., 2022).

Although efforts have been made to build cybersecurity programs, research indicates a significant gap between classroom instruction and the realities of the cybersecurity profession (Yang, 2021). According to Zafar et al. (2024), academic institutions tend to favor concepts over practical abilities, even though practical experience is essential. Even competent users who were familiar with Cybersecurity rarely used it in practical settings (Zwilling et al., 2022). Disparity is mostly caused by university programs that prioritize academic knowledge over practical experience, and the speed at which cyber dangers are evolving ahead of curriculum development.

Additionally, research has shown that college students lack a comprehensive understanding of Cybersecurity. At Saudi University, students lacked awareness of data protection measures, indicating a deficiency in their cybersecurity expertise (Alotaibi et al., 2021). In addition, a study conducted at a Nigerian college found that although some students demonstrated a basic understanding of Cybersecurity, they still lacked knowledge of data protection (Catal et al., 2023; Dawson et al., 2022). Therefore, this indicates that college students lack a thorough understanding and adaptability in cybersecurity measures.

Several studies highlight the benefits of experiential methods. It shows that possessing the experience not only deepens understanding but also enhances behavioral readiness and competence, a critical component for criminology students as they focus more on lived experience, perceived competence, and actual application of cybersecurity measures. Systematic reviews show that learner-centered strategies improved motivation, comprehension, and hands-on abilities (Ahmed et al., 2024). Studies demonstrate that virtual laboratories, simulations, and gamified virtual exercises increase learners' self-efficacy and conceptual understanding. Empirical research finds that several universities have students who remain vulnerable to phishing. A test conducted shows that 70%-90% of students unconsciously open and engage with at least one phishing email, indicating substantial awareness among students towards Cybersecurity (Morrow, 2024).

David A. Kolb's Experiential Learning Theory (1984), which explains that students learn more efficiently when they actively and fully engage in the learning process rather than simply listening to lectures, serves as the main foundation of this study. According to the theory, learning becomes more meaningful when students gain experience, reflect on it, and apply what they have learned to real situations. This can be achieved in cybersecurity education through exercises that allow students to test their skills, such as case studies, laboratory activities, simulations, and problem-solving assignments. These educational opportunities can enhance their understanding of cybersecurity principles and help them develop the practical skills needed to identify and address cyber threats. Using interactive teaching techniques can promote digital awareness, reasoning skills, and responsible online behavior since active engagement also enhances students' comprehension and retention of information.

In addition, this study is supported by Social Cognitive Theory, proposed by Bandura (1986), which explains that learning is influenced by observing others, social interaction, and modeling appropriate behaviors. According to this theory, individuals acquire new knowledge and behaviors by observing others and applying what they learn to their own experiences. This theory presents how personal cognitive factors, behaviors, and environmental influences interact reciprocally. Social Cognitive Theory also explains that people’s confidence in their ability to perform a task can influence how well they learn and apply new knowledge (Bandura, 1997). SCT supports the use of teaching strategies that allow criminology students to observe and participate, providing opportunities to learn from others and engage in practical activities needed to respond to cybersecurity challenges. These teaching approaches are especially beneficial because the field of cybercrime continues to evolve, requiring students to adapt to new threats. The study is further supported by Lave and Wenger's Situated Learning Theory (1991), which holds that learning becomes more meaningful when students actively participate in real-world contexts and work with others. In accordance with ELT, students gradually build their knowledge, confidence, and skills through meaningful experiences that reflect actual practice. In this course, this can be attained through scenario-based learning, which may prepare criminology students to respond to real-world cybercrime scenarios.

Experiential learning platforms designed for Cybersecurity can increase student engagement and help develop practical skills. Despite these benefits, these platforms are not yet widely used in some academic fields, especially in criminology, where students have limited opportunities for such hands-on cybersecurity training (Vaish et al., 2024). Besides that, teacher preparation is the primary issue when presenting cybersecurity concepts at the school level. They should ensure that their students learn the new material and develop the skills they need by using modern delivery approaches enhanced with interactive resources, such as educational games (Blažič & Blažič, 2025).

The demand for cybersecurity education has led to a need to enhance teachers' abilities and develop creative strategies to better teach Cybersecurity to the workforce of the future (Ayanwale, 2024). The teaching methodology is not aligned with the demands of contemporary teaching and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

sustainable education (Burns et al., 2023; Cybersecurity Europe, 2022). University courses and training programs in a variety of subjects, including ICT, intended to prepare high school teachers are still heavily technocratic, according to studies (Angafor et al., 2020). This study addresses this knowledge gap by focusing on the University of Mindanao Main Campus's criminology department to assess and enhance the school's instructional strategies and practices in teaching Cybersecurity to aspiring law enforcement professionals.

This research aims to explore the strategies educators use to teach cybersecurity measures to criminology students. Specifically, the study seeks to 1) identify teaching strategies currently employed within the criminology program to deliver cybersecurity instruction; 2) it also examines how students perceive and respond to these strategies, focusing on their engagement, understanding, and ability, to apply what they learn; 3) The study explores the challenges criminology students encountered when learning cybersecurity topics, as well as 4) how they apply cybersecurity concepts and digital investigation skills acquired in the classroom to real-world or simulated cybercrime scenarios.

The results of this study can support leadership in developing security awareness initiatives that promote more effective and inclusive cybersecurity education for students. The engagement of both program leaders and students in cybersecurity education reflects the growing importance of strengthening Cybersecurity learning in criminology, making this relevant to the field (Hobbs, 2023). This study helps develop an improved cybersecurity curriculum for criminology programs by enabling students to learn more about Cybersecurity and prepare to address cybercrime. Apart from that, it supports the Sustainable Development Goals, also known as SDGs, of the United Nations, such as SDG 16 Peace, Justice and Strong Institutions, which promotes cybersecurity awareness and crime prevention in the modern era, and SDG 4, which is about Quality Education to ensure students experience quality learning in the field of cybersecurity education. The results may also help educators improve cybersecurity courses and better equip upcoming law enforcement officers with the extensive understanding and skills needed to respond to emerging cyber threats.

Several restrictions and boundaries define the scope of this study. The small number of respondents from the few institutions that offer criminology programs is a drawback. The results might not accurately reflect the experiences of every criminology student. The study's limitation aligns with the qualitative phenomenological research design selected, which focuses on comprehending participants' lived experiences rather than generating results that can be extrapolated to a larger sample. Additionally, this study uses self-reported data, which participants' viewpoints and experiences may influence. The researchers employed semi-structured interviews with a standard interview guide to improve the data's coherence and credibility.

This method ensured that the data gathered aligned with the study's goals while enabling participants to explain their experiences in their own words. The variety of information obtained might have been affected by the short data-collection time frame. Despite this, the researchers managed to gather sufficient, pertinent data to meet the research objectives. The study's scope is limited to specific criminology students and graduates of the Bachelor of Science in Criminal Justice Education program who have completed a Cybersecurity course. It focuses particularly on instructional techniques and student learning experiences in cybersecurity education. It uses only qualitative, semi-structured interviews to gather data, excluding other educational initiatives, establishments, and research methods outside the study's specified scope.

II. METHOD

This section presents the research design, research respondents, study locale, research instrument, data collection, data analysis, limitations and delimitations, and ethical analysis.

- *Participants of the Study*

The sample consisted of 8 students from 2 universities that offer the Bachelor of Science in Criminal Justice Education, exploring meaning in depth rather than generalizing from statistics (Vanover, 2022). The inclusion criteria required that students or graduates be enrolled in the Bachelor of Science in Criminology program and have completed or were currently enrolled in cybersecurity-related courses. However, to ensure sample relevance and voluntary participation, students who are not enrolled in the program, have not taken cybersecurity-related subjects, or are unwilling to participate are excluded.

Purposive sampling was used to identify respondents who were familiar with the teaching and learning processes in cybersecurity education within the Bachelor of Science in Criminology program. Using this non-random approach, instances that offer rich, detailed data are selected to provide a thorough understanding of the topic being studied (Campbell, 2020). This study selected students as respondents based on their participation in the phenomenon to gain firsthand experience and extract rich, meaningful insights (Fouché et al., 2021).

The selection of study participants was based on the inclusion of students or graduates of the Bachelor of Science in Criminal Justice Education who were currently taking or had previously taken Cybersecurity courses. Students who were not enrolled in the criminology program, did not respond to the questions, or did not want to participate were not included in the study. Participants were assured that the study was voluntary and that they could discontinue participation at any time without penalty or consequences.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

Table 1 Respondents' Profile

Codename	Education Level
C1	4th year Student
C2	4th year Student
C3	4th year Student
C4	4th year Student
C5	4th year Student
C6	3rd year Student
C7	Graduate
C8	Graduate

➢ *Material and Instruments*

This study employed a qualitative phenomenological design, using a semi-structured interview guide as its primary research instrument. An interviewer guide was developed to provide a flexible structure for deeper exploration of important responses while allowing respondents to freely communicate their lived experiences. Using semi-structured interviews allowed the researchers to focus on the study's main topics while also exploring new ideas that emerged during the interviews (Ruslin et al., 2022). The interview guide was prepared by the researchers, with guidance from their research adviser, to ensure the questions aligned with the study's objectives and focused on participants' cybersecurity learning experiences. The study used in-depth interviews to collect data on participants' feelings, perceptions, and personal meanings associated with their experiences (Osborne & Grant-Smith, 2021).

In-depth interviews support the phenomenological goal of understanding respondents' experiences in their natural context. The interview was conducted using the respondent's comfortable language, which was Cebuano/Visayan, Filipino, or English, to ensure comfort, clarity, and legitimacy of responses. Respondents were asked for consent to record audio for accurate transcription and analysis. Consistent with qualitative practices focusing on the essence of capturing nuanced verbal expressions (Vanover, 2022). In summary, the use of semi-structured guide questions and in-depth interviews ensured that the collected data aligned with the study's exploratory nature.

➢ *Design and Procedure*

The phenomenological research approach was primarily employed to rasp social phenomena from respondents' perspectives (Fouché et al., 2021), so the researchers decided to adopt an exploratory research design. Exploratory research is a study that provides in-depth insights and context, enabling researchers to develop a more comprehensive understanding of intricate events (Aithal & Aithal, 2023), making it a suitable approach for investigating criminology students' perspectives. Additionally, purposive sampling guided the researchers in selecting respondents who were competent in the teaching and learning experience in cybersecurity education. This method is intended to provide researchers with thorough knowledge of the topic they are researching (Thomas, 2022), ensuring that respondents align with the study's objectives.

The researchers had different roles in conducting this study, assigned to specific tasks for data collection from respondents. The following responsibilities and steps were established to maintain the procedures organized. The first was the interviewer, who performs semi-structured and structured interviews. After obtaining the respondent's consent, a questionnaire interview guide was used, which included a set of pre-formulated questions. To facilitate open-ended responses and encourage the respondents to expand on their initial responses, follow-up questions were posed. Comprehensive data that offers an understanding of a person's perspective, experiences, feelings, and the importance they place on a certain subject or problem.

Then there was a transcriber. Following each participant's interview, their answers were encoded from the audio recording with consent. Interview transcription used for both data collection and analysis. To better understand the material they investigate, researchers listened to and watched recordings of their interviews and wrote based on that information, verifying its accuracy and helping develop the reliability and validity of the research (Vanover, 2022). Third, a translator. Since standard English is a commonly accepted language for scholarly papers, it was used to translate the transcription after it was completed, ensuring a wider dissemination of knowledge.

The researchers followed several important guidelines to ensure the study's credibility. First, aligning the research findings with reality enhanced credibility. Triangulation, which uses multiple sources of information to identify recurring patterns, was used because credibility is inherently subjective. Then, dependability and reliability were preserved by actively fostering trust in the research and expecting peer review as an indicator of dependability. Keeping the research as close to objective reality as feasible was the third goal of objectivity. Throughout the trial, the researchers prioritized procedures that improved accuracy and precision. Unlike other methodologies, thematic analysis understands the complexity and context-specific variation.

This study adhered to the established ethical standards to ensure the protection, privacy, and wellbeing of all respondents. By explaining the study's goal and participants' right to withdraw at any time, voluntary participation is ensured.

Respondents were informed, asked for their consent, provided with clear, non-technical instructions about the study, and assured of the confidentiality of the data extracted. To maintain the integrity and ethical conduct of the research process, researchers also proactively identify and mitigate potential ethical issues related to technology, authorship, dishonesty, deception, conflict of interest, plagiarism, fabrication, falsification, and the ethical conduct of data collection methods (Agbakhamen, 2025).

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

The collected data were analyzed through a thematic analysis. The researchers repeatedly reviewed the interview transcripts to gain a thorough understanding of the participants' responses. Meaningful statements were coded, grouped into related categories, and organized into themes based on the participants' lived experiences. These themes were then interpreted to identify a common pattern and address the objectives of the study.

By using a methodological approach for data collection and analysis, the study guaranteed integrity. To maintain accuracy and consistency, the researchers were assigned specific tasks, such as conducting interviews, transcribing responses, and translating data. By obtaining participants' informed consent, maintaining confidentiality, and highlighting voluntary participation, ethical standards were upheld. The study's theoretical framework, in particular Experiential Learning Theory as the anchor theory, and Social Cognitive Theory and Situated Learning Theory as supporting theories, provided a solid basis for comprehending the participants' experiences and for interpreting the results. Despite the research's small sample size, these steps enhanced the reliability and validity of the findings.

III. RESULTS AND DISCUSSIONS

The study's results, derived from interviews with students and graduates studying criminology, are presented in this section. It investigates their experiences with cybersecurity education, including the instructional methods used, the application of acquired knowledge, and the tools at their disposal. The study's research objectives are used to organize the findings, which are bolstered by participants' responses.

A. Teaching Strategies in Cybersecurity Instruction among Criminology Students

Based on criminology students' experiences, this section presents findings on the teaching strategies employed in the courses. Their answers shed light on how cybersecurity ideas are taught and how these teaching strategies enhance students' learning. This document presents the different teaching strategies and classroom practices that influence students' learning experiences through the author's personal perspective.

Table 2 Themes on Teaching Strategies in Cybersecurity Instruction among Criminology Students

Themes	Significant Statement
Theory-Guided and Practical Learning Approaches	Effective for our learning, as it is a practical application of legal concepts. [C2] They integrate by explaining the theoretical concepts and giving examples, like in the news and past similar situations [C7]
Lecture-Based Instruction as the Primary Method	These lecture-based instructions are the most common. The purpose is to build a theoretical foundation, so it is commonly used to teach subjects like cybercrime laws. [C6] The most frequently used instructional methods are likely lectures and case analysis. [C7]
Use of Multimedia-Based Instruction	Technology is incorporated into cybersecurity instruction by allowing students to apply their theoretical knowledge through real-life or simulated digital tools. [C6] These virtual laboratories include virtual machines, sandbox environments, and simulated attack scenarios. The tools commonly used in these activities are Kali Linux and VMware. [C6]
Application-Driven and Collaborative Learning	Incorporating these shared experiences into my classes is a very big help because of the knowledge they can provide and the experience that can enhance our overall capabilities in Cybersecurity. [C4] My instructor focused on problem-based learning and group work, which encouraged teamwork, communication, and problem-solving skills. [C8]
Limited Hands-On and Technology Integration	More on the theoretical side, which is by the book; it has little exercise. [C2]

➢ *Theory-Guided and Practical Learning Approaches*

Respondent always indicated that their learning experience was both theoretical and practical. Several students reported that they are taught cybersecurity concepts, and only later do instructors give examples in real-life scenarios such as cybercrime cases, phishing, and violations of the law. Other respondents also noted that lessons are linked to investigative practices, as they learn how theories are applied in the field.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

"..effective ang learning namo since practical man gud siya na applications with legal concepts." (C2)

...learning was most effective because of its practical applications with legal concepts.

This strategy indicates that teachers are trying to close the knowledge-practice gap. Through a combination of theory and practice, students can better understand abstract concepts and observe how they apply in real-life cybersecurity scenarios. McLeod (2025) on Kolb's Learning Style and Experiential Learning Cycle states that learning would be more meaningful when students can put what they have learned into practice. Even basic examples and discussions of real cases are useful, as they can help students build a deeper understanding of Cybersecurity. In addition, according to Kashyap et al. (2025), experiential learning enables students to better understand cybersecurity concepts by allowing them to apply theories in simulated or real-life scenarios. Likewise, Raffaghelli et al. (2022) stressed that combining theoretical instruction with real-life case scenarios enhances students' problem-solving abilities and long-term knowledge retention.

- *Lecture-Based Instruction as the Primary Method*

Students have said that there is a tendency for instructors to combine theoretical material and practical examples. Nonetheless, the majority of them stressed that lecture-based teaching is the most common mode of teaching. Multimedia tools (PowerPoint presentations, video outputs) are used regularly, and collaborative and application-based activities are sometimes included. Though these were done, many students reported that the availability of practical activities and technological equipment was limited. The respondents quoted:

"We use blended learning and a case study to teach students more effectively, and we can use it in the real world. So, among the common methods are lectures or delivering foundational knowledge" (C1)

We use blended lectures and a case study to teach students more effectively and to help them apply what they learn in the real world. So our common method is lectures or the delivery of foundational knowledge.

"Ang pinaka primary gud is lectures. Since mao gud ng murag backbone sa pagtudlo." (C2)

The primary method used is lectures, as they serve as the backbone of instruction.

The findings are consistent with previous studies, indicating that lecture-based instruction remains effective for introducing complex cybersecurity concepts. The data support the studies of Shivapurkar et al. (2020), suggesting that lecture-based instruction remains effective for introducing complex cybersecurity concepts. However, their effectiveness improves when combined with interactive activities. Similarly, relying solely on lectures may reduce students' engagement, underscoring the need for participatory teaching strategies. These findings suggest that while conventional lectures are useful for introducing concepts, they may limit student interaction when used alone. Thus, in this study, students' perception of cybersecurity education as primarily theoretical may have been influenced by the frequent use of lectures.

- *Use of Multimedia-Based Instruction*

According to the respondents, cybersecurity education involved virtual tools like software demonstrations and simulated environments. These resources were not consistently used across classes, suggesting that different learning activities involved varying levels of technology integration. Technology is occasionally incorporated by discussing digital tools in Cybersecurity, such as forensic software or virtual machines. C1 and C4 mentioned that:

"So technology is used in various ways, such as utilizing digital forensic tools to teach investigative techniques and using this software for hands-on learning and tools." (C1)

"..the most frequently used method in my cybersecurity classes was..video presentation, recorded presentation, or PowerPoint presentation." (C4)

Multimedia enhances the learning process by making lessons more interactive and easier to comprehend. According to Kurt and Kurt (2024), multimedia learning can help students process information more efficiently by incorporating both visual and auditory components. This is especially true in Cybersecurity, where the concepts can be very technical and abstract. In line with this, one study found that multimedia learning enhances learning by allowing students to process information. simultaneously in both visual and auditory modes (Shillair et al., 2022). In addition, it is established that video-based and digital learning have a significant effect on enhancing understanding of technical and abstract ideas in information technology courses (Dahlan et al., 2023).

- *Application-Driven and Collaborative Learning*

The outcome also shows that some teachers employ collaborative and application-oriented learning techniques. The respondents described engaging in group activities, problem-solving tasks, and discussions of real cases. These learning experiences encouraged active participation and enabled students to apply their cybersecurity knowledge to practical and real-world situations.

"My instructor focused on problem-based learning and group work, which encouraged teamwork, communication, and problem-solving skills." (C8)

"Nagagamit syag example na naga-connect lang sya sa real-world ug nagamit namo sya, and also the discussion relate-classroom concept" (C1)

They use examples that connect to real-world situations, and we can apply them as well. The discussion concerns classroom concepts.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

This type of learning is very much in line with constructivist principles, as students learn through interaction with the material and with others. To enhance the learning process, Zajda's (2021) study found that authentic learning conditions, including real-world activities and group work, help students acquire deeper knowledge and transferable skills. This is supported by Kalukar et al. (2024), who found that problem-based and collaborative learning enhance students' critical thinking and real-world preparedness.

- *Limited Hands-On and Technology Integration*

One of the most striking findings is that application activities and technological tools were not prevalent in cybersecurity courses. Several respondents reported that they are mostly taught Cybersecurity through textbooks, lectures, and PowerPoint presentations and have not been exposed to real-world cybersecurity tools, lab sessions, or simulations. The respondents expressed this challenge:

"Wala man mi ginagamit na tools so kuan lang jud siya book to book basis, like tudlo lang ang terminologies, meanings so.. mao lang" (C3)

Since we don't really use any tools, it is really just on a book-to-book basis, like just teaching the terminologies and meanings, so that is just it.

"cyber applications wala kaayo mi naka kuan ana since na mention nako earlier nga walay laboratory activities ang cybercrime nga topics or subject" (C2)

Cyber applications were not widely used because, as mentioned earlier, there were no laboratory activities in the cybercrime subject.

Hands-on learning is a crucial element of cybersecurity education because it allows students to develop technical skills and gain experience. Mukherjee et al. (2024) also propose that excellent cybersecurity training should include simulations, labs, and practice to prepare students for professional practice. Research emphasis is on hands-on exposure. Alzahrani et al. (2021) found that learners with limited access to laboratory tools struggle to acquire the necessary cybersecurity skills. On the other hand, Dutchatelet et al. (2020) noted that providing students with real-world learning experiences and simulation-driven learning environments supports the development of practical technical skills.

B. Students' Perception and Responses to Cybersecurity Teaching Strategies

Students' views and reactions to cybersecurity teaching strategies reveal how these strategies affect their interest in and comprehension of the subject. Different teaching approaches, such as lecture-based, multimedia-supported, and collaborative learning, shape their experiences and influence their understanding and engagement in the learning process. In cybersecurity education, interactive and collaborative strategies help students deepen their understanding, improve their critical thinking, and apply cybersecurity concepts in practice.

Table 3 Themes on Students' Perception and Responses to Cybersecurity Teaching Strategies

Themes	Significant Statements
Application of Cybersecurity Concepts in Real-Life and Investigative Contexts	One activity involves analyzing cases; this activity helps Cybersecurity, such as data security and cybercrime identification. [C1]
Personal Digital Security and Preventive Practices	Use a two-factor authenticator and physical barriers to protect your accounts on your personal computer. [C2] So techniques like cyber investigation, one of the first of which is our email analytics technique, examine email messages to identify IP addresses. [C6]
Awareness and Preventive Cybersecurity Practices	So it is really beneficial to understand cybercrime. [C4] The teaching strategies you learn help you protect your digital, personal information and privacy by helping you understand how cybercrimes are committed and how to prevent them. [C7]
Limited Hands-On Skill Development	For skills, maybe I did not gain any since it was more for awareness only and learnings that can be applied basically [C3] It was only in the textbook because we did not have, or it did not have, any lab activity [C1]
Case Analysis as a Tool for Practical Cybersecurity Learning	When there is a case analysis, I can broaden what I know, like how to counter malware [C3]
Experiential Learning Through Simulations	Hands-on activities help you understand actual procedures through hands-on learning. It provides guidelines you can follow and helps you understand the process and how to carry it out. [C7]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

➢ *Application of Cybersecurity Concepts in Real-Life and Investigative Contexts*

The criminology respondents indicated that teaching strategies will help them connect classroom lessons with real-life cybercrime situations. By discussing cases and giving examples, students will be able to understand how cybercrimes, such as phishing, hacking, and identity theft, occur and can be investigated. The respondents said that:

"Lecture-based instruction and classroom activities helped me apply cybersecurity concepts to real-world cybercrime and investigative scenarios in practical ways…we may examine a cybercrime scenario, identify how the attack happened, and suggest ways to prevent it." (C8)

"There are specific activities and lessons where I applied cybersecurity concepts to a real or simulated cybercrime, such as if I forget my password through the concepts of cybercrime, like links between phones of other applications" (C4)

This result suggests that cybersecurity education goes beyond theoretical understanding to the growth of awareness of the abrupt situations and analytical abilities. Ainslie et al. (2023) found that case-based learning improves students' decision-making in realistic cybersecurity situations, while Ahmed et al. (2024) reported that context-based learning enhances the application of knowledge to real-world settings, enabling them to adapt in sudden situations.

➢ *Personal Digital Security and Preventive Practices*

The other significant result is that students use cybersecurity knowledge in their own digital practices. A significant number of them claimed to have used two-factor authentication, not clicked on suspicious links, protected their accounts, and engaged in safe browsing. The respondents stated that:

"ang pinaka nagamit gud namo is more on physical like if ever mag gamit ka ug public computer dili nimo siya pasagdan or siguraduon gud nimo then use incognito. Nagbuhat mi ug murag instructional video on..sa akoa topic nako How to Secure your Account." (C2)

What we really focused on most is the physical side: if you're using a public computer, don't just leave it unattended; make sure to secure it, then use incognito.

"In digital forensics pud kay ma-exercise nato ang atong mga important sa mga evidence like handling, chain of custody ug accurate preserving para ma-realized ang mga small mistakes sa paghandling sa digital data coming from the outcome of the case." (C6)

In digital forensics, we practice important aspects such as evidence handling, chain of custody, and proper preservation, so we can identify even small mistakes in handling digital data and their impact on case outcomes.

This means that cybersecurity training is effective in influencing students' behavior outside the classroom. According to a recent study, cybersecurity awareness campaigns may be effective in promoting behavioral change and reducing risk among students (Sarita et al., 2024). This is supported by Bada and Nurse (2020), who found that cybersecurity education can improve students' online safety behaviors. The research revealed that awareness initiatives may lead to quantifiable changes in how people protect their personal information.

➢ *Awareness and Preventive Cybersecurity Practices*

Cybersecurity awareness is closely connected with personal practices. The respondents said that they are more aware and careful of online threats. They recognize phishing, suspicious links, and unsafe internet behaviors.

"The teaching strategies that you learn help you protect your digital, personal information and privacy as it helps you to understand how cybercrimes are committed and how to prevent them." (C7)

One of the best methods of mitigating cybersecurity risks is through increased awareness, as stated by Shillair et al. (2022). Moreover, as Alshaikh (2020) noted, human awareness is the first line of defense against cyber threats. This aligns with the literature, which emphasizes awareness as a precondition for cybersecurity training, especially for beginners. Awareness-based learning enables students to understand the hazards of the digital environment and be ready to take on responsibility (Alnajim et al., 2023).

➢ *Limited Hands-On Skill Development*

Despite the positive results in awareness and application, students indicated that they had not developed technical skills to a great extent. The majority of respondents said they study through lectures and discussions and have limited access to tools, software, and laboratory work. C5 and C3 expressed their experience in classes, and quoted:

"Since wala mi activity kaayo gibuhat uhm.... wala mi mga softwares na gigamit wala pud mi tools na gigamit ah.. techniques nuon gidiscuss pero wala wala pud lage nagamit so, mao rato." (C5)

Since we didn't really do many activities, we also didn't use any software or tools. Ah… the techniques were discussed, but they weren't actually put into practice. So, that's all.

"Since dili pud ko tech-savy, awareness lang pud jud ang maprovide sa professor namo personally." (C3)

Since I am not very tech-savvy, our professor mainly provides us with awareness, personally.

Such a limitation is what introduces a knowledge-practice gap. Khando et al. (2021) support this weakness by concluding that a lack of practical experience undermines students' technical competence in Cybersecurity. This paper underscores the importance of experiential training for acquiring problem-solving and technical skills. It has been shown that hands-on training is essential in cybersecurity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

training, as it helps students develop problem-solving and technical expertise (Ahmed et al., 2024).

- *Case Analysis as a Tool for Practical Cybersecurity Learning*

Case analysis was one of the most commonly used strategies that helped students apply cybersecurity concepts. Students are taught to think critically and conduct research by analyzing real or hypothetical cases of cybercrime.

"pag naay case analysis kay mas ma broaden nako ang akong nahibal an like how to counter malwares." (C3)

When there's a case analysis, I get to learn more, like how to counter malware.

Case-based learning improves students' analytical thinking skills by exposing them to real-life issues (Silitubun et al., 2025). The latter is supported by the research of Kaur et al. (2023), which establishes that case studies in Cybersecurity enhance students' ability to assess threats and provide effective solutions. It is a technique that can be attributed to problem-based learning, in which students participate in the process of problem-solving and proposing solutions to real-life problems. Case-based methods have been established to boost analytical skills and knowledge in cybersecurity education (Lazarov et al., 2025).

- *Experiential Learning Through Simulations*

Other respondents had participated in simulations such as phishing and digital investigation exercises. These activities allow students to engage in learning by doing, which enhances learning. C7 mentioned that:

"A phishing awareness simulation was one of the classroom exercises that helped me gain useful cybersecurity skills. After creating a false email threat, our teacher instructed us to look for indicators that it was a phishing assault. We looked at the sender's address, suspicious connections, and grammatical mistakes." (C7)

"Hands-on activities help by providing experience and guiding us through investigative steps such as identifying evidence and analyzing digital data, which improves our understanding of real investigative procedures and broadens our learning further." (C1)

It is not a secret that experiential learning is among the most effective approaches to teaching cybersecurity, as it allows students to apply theoretical knowledge in practical contexts (Mukherjee et al., 2024). Students can hone their critical thinking and problem-solving abilities through practical exercises such as lab work, case analysis, and simulations. This viewpoint develops both theoretical knowledge and practical proficiency, equipping students to handle the digital problems encountered in the real world. In a similar vein, Marougkas et al. (2023) clarified that simulation-based and immersive learning environments enhance situated learning. Through investigative exercises and phishing simulations, students can gain an applied knowledge of Cybersecurity and improve their problem-solving abilities by engaging directly with real-world situations.

C. Challenges Faced by Criminology Students in Learning Cybersecurity Measures

Learning cybersecurity measures poses many difficulties for criminology students, especially when it comes to understanding intricate legal and technical concepts. Their capacity to completely understand and apply the material is further hampered by limited access to digital resources and a lack of opportunities for hands-on learning. These limitations reduce opportunities for active participation and progressive skill development. Addressing these challenges is important to help learners achieve a more comprehensive understanding of Cybersecurity.

Table 4 Themes on the Challenges Faced by Criminology Students in Learning Cybersecurity Measures

Themes	Significant Statement
Complexity of Cybercrime Law and Technical Concepts	In the lessons that were discussed, I had difficulty understanding cybercrime offenses because there are many sections. I also had difficulty with cybercrime warrants. These challenges made it harder to learn about cybercrime. [C1] In cybersecurity, the hardest part is the legal basis, because you can't be careless. [C2]
Limited Digital Resources and Device Accessibility	The limited devices for all activities. It is challenging to make it work due to limited resources, like PC [C4] Understanding and using properly, like software use, network monitoring, and digital forensics, can be challenging, and I took time to learn how to navigate and analyze the results accurately [C6]
Limitations of Learning Resources and Hands-On Tools	The learning resources were probably books and PPTs only because those were what we had access to. [C3] The challenges I encountered during hands-on activities were grasping the concept and applying it in practice. [C7] Limited time and resources to make a careful analysis of all the data make it much more challenging. [C8]

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

➢ *Complexity of Cybercrime Law and Technical Concepts*

The respondents indicated that they were struggling to understand cybersecurity matters, particularly the law and terminology. The laws of cybercrime, network protocols, and digital forensics were described as complex and difficult for students to grasp. C6 quoted that:

"I experience several challenges especially mga understanding in technical concepts ug mga pag-apply sa mga practical situation. So daghan mga terms sa cybersecurity but such as mga inscription or mga network protocols like mga IP tracing ug kaning digital forensic so kani, it is really difficult to understand or dili man jud ni sya masabatan ning mga ginagamit ba" (C6)

I experience several challenges, especially in understanding and applying technical concepts in practical situations. There are many cybersecurity terms, such as encryption, network protocols, IP tracing, and digital forensics.

Cybersecurity is an interdisciplinary field combining law, technology, and investigation. Oroni et al. (2024) support this by reporting that students struggle to grasp concepts due to the technical and interdisciplinary nature of Cybersecurity. This complexity can overwhelm the students, especially those who are not well prepared technologically. Cybersecurity education is challenging for many students, especially when dealing with complex topics such as cybercrime offenses and legal issues. The assimilation of technical and legal concepts makes Cybersecurity challenging for students with limited background knowledge. Similarly, Ghuzali et al. (2024) reported that students are more likely to experience hardships in learning Cybersecurity when they lack foundational knowledge and prior exposure to technical concepts.

➢ *Limited Digital Resources and Device Accessibility*

A lack of devices or shared resources has been cited by other students who have reported problems with participation in activities. Another significant challenge identified was the limited access to digital resources, including computers, software, and laboratory facilities.

"It is hard, especially when you have no appropriate device to experiment and do all the activities…so even though I have limited devices on hand, I still figured it out how to make it work." (C4)

An important area of cybersecurity education is access to technology. Without the right tools, students cannot practice and experiment, which in turn affects their learning. The research emphasizes that to pursue digital and technical education, access to technology is essential (Ahmed et al., 2024). Altarawneh et al. (2025) state that access to digital tools is limited, hindering successful learning, particularly in technology-based courses. It is observed that the inaccessibility of devices and the internet significantly influences students' learning experiences.

➢ *Limitations of Learning Resources and Hands-On Tools*

The other point raised by the respondents is that they can only learn through textbooks, PowerPoint presentations, and lectures. A lack of practical tools, simulations, and lab activities impedes their understanding and practical implementation of cybersecurity concepts.

"Ang gi provide lang saamoa kay katong tong...PPT rajud namo wala mi tools so nagklase lang jud mi, lectures unya maghatag ug assignments online mao rato." (C5)

What was provided to us was just… the PPT. We didn't have any tools, so we just attended class, listened to lectures, and completed assignments online. That's all.

Modern cybersecurity education focuses on virtual labs, cyber ranges, and simulation tools to support learning. Prümmer et al. (2023) support this by the fact that the lack of practical tools hinders the development of skills in cybersecurity education. That laboratory-based learning is important in comprehending technical concepts should be supported. In the absence of these resources, students can struggle to acquire the technical skills they need (Mukherjee et al., 2024).

D. Application of Cybersecurity Concepts and Skills in Real-World or Simulated Scenarios

The practical significance of the subject is demonstrated by the application of cybersecurity concepts and skills in real-world or simulated circumstances. Students' analytical and problem-solving skills improve when they can relate theoretical information to real-world circumstances. Despite this, experiential and scenario-based learning approaches offer valuable opportunities to reinforce practical competencies.

Table 5 Themes on the Application of Cybersecurity Concepts and Skills in Real-World or Simulated Scenarios

Themes	Significant Statement
Practical Usefulness of Cybersecurity Knowledge	What I learned in Cybersecurity regarding cybercrime was really useful. [C5] We can apply the concept of Cybersecurity and digital investigation skills through behavioral analysis, forensic laboratory work, handling cases like phishing, ransomware, and financial fraud [C4]
Cultivating Cybersecurity Awareness and Safe Online Practices	It prepares me to be wise and have knowledge to know the consequences of every little thing on cyberspace [C4] Do not connect to public Wi-Fi carelessly. [C2]
Application of Classroom Activities to Real-World Scenarios	The classroom activities prepared me by teaching me how to handle these situations [C7] In our classroom, we were made to do exercises like phishing case scenarios. [C6]

➢ *Practical Usefulness of Cybersecurity Knowledge*

The respondents admitted that the knowledge gained can be applied in the real world, particularly in the following areas: digital investigation, evidence handling, and cybercrime prevention.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

"Apply the cybersecurity concepts by avoiding the practice that could cause cybercrime" (C7)

"..pag investigate ug pagresponse cybercrime cases..pagkuha sa mga documents or mga importance na files sa computer ug kaning mga ransom ware ug kaning mga online threats" (C6)

..investigating and responding to cybercrime cases..getting documents or important files from a computer, ransomware, and online threats.

This implies that cybersecurity training is part of professional readiness and preparedness, especially among criminology students who may work in law enforcement or investigations. In one study by Abrahams et al. (2024), it is noted that cybersecurity education enhances students' preparedness for professional work by cultivating applied skills. However, another study emphasizes that structured cybersecurity training frameworks facilitate the development of competency (Nasir, 2023). Research supporting this claim is that implemented cybersecurity training enhances occupational preparedness and applied capability (Mukherjee et al., 2024).

- *Cultivating Cybersecurity Awareness and Safe Online Practices*

Students said that they were more careful in their online activities, including not clicking on suspicious links, creating accounts, and keeping their personal information safe. C4 stated that:

"When sharing information, you should be responsible for what you share on social media; it is a platform that the public can see and criticize …So, it's better to think before you click. It prepares me to be wise and have knowledge to know the consequences of every little thing on cyberspace." (C4)

This aligns with Khando et al. (2021), who found that cybersecurity education affects safer internet practices. Also, this demonstrated that the higher the awareness, the less risky digital practices users engage in. Education on Cybersecurity is important in fostering safe online behaviors and minimizing susceptibility to cyber threats (Sarita et al., 2024). Such behavioral shifts are necessary, particularly in today's digital world. Additionally, this result is consistent with Bandura's Social Cognitive Theory (1986), which explains how people develop behaviors through observation, experience, and environmental influences. Students gained more awareness and safer online behavior for guarding their digital activities and personal information through cybersecurity class discussions.

- *Application of Classroom Activities to Real-World Scenarios*

Respondents emphasized that classroom activities, such as case studies, simulations, and assignments, help them prepare to encounter real-life situations. These activities will help them to apply theoretical knowledge to practical situations.

"gi-relate lang nako tong mga assignment sa real-life examples mao ra giapang-relate lang nako to katong mga topics, lectures uhm..practical examples. Gi relate lang nako" (C5)

I just related the assignments to real-life examples. I only connected them to the topics, lectures, uhm..practical examples. I just related them.

Another active learning technique that has been demonstrated to enhance knowledge and skills in Cybersecurity is project-based and simulation-based learning. (Ahmed et al., 2024). To reinforce this, one study found that project-based learning enhances students' ability to apply knowledge to real-world contexts (Schumacher & Ifenthaler, 2020). The importance of underlining is highlighted by the fact that applied learning and skill transfer are enhanced through simulation-based activities.

IV. IMPLICATION AND CONCLUDING REMARK

This study explored the teaching strategies, learning experiences, challenges, and real-world applications of cybersecurity education among criminology students. The study's findings showed that learning is more efficient and effective when theoretical knowledge is supported by practical and experiential activities, despite teachers' use of a combination of multimedia, lecture-based, and application-based approaches. Skill development is still constrained by few opportunities for hands-on training and limited access to laboratories and technological resources. Despite these difficulties, students demonstrated a greater understanding of Cybersecurity and the ability to apply their expertise in both investigative and daily settings. These results stress the need for more firsthand cybersecurity training.

- *Implication for Practice*

The implications of this study highlight the importance of combining theoretical instruction with hands-on, experiential learning strategies in Cybersecurity courses. The findings show that students gain deeper comprehension when learning is reinforced through case analysis, real-life examples, and practice exercises, even though lecture-based instruction remains crucial for imparting fundamental knowledge. The Experiential Learning Theory of David A. Kolb (1984), which holds that meaningful learning occurs when students actively engage in and reflect on practical experiences, lends credence to these findings. To encourage the application of theoretical concepts in practical cybersecurity contexts, the findings recommend that educators adopt more interactive, student-centered strategies. These methods could further improve students' knowledge, logical reasoning, problem-solving skills, and readiness for future careers.

To address this issue, educational institutions might consider adding more laboratory-based activities or offering Cybersecurity as a laboratory course. This would give students hands-on training in digital investigations, cybercrime analysis, and the use of pertinent cybersecurity

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

software and lab manuals. Students may have fewer opportunities to acquire the technical skills necessary to supplement their stock theoretical knowledge due to the limited use of tools and exercises in this course. The results of this study also aim to emphasize the need to improve experiential learning opportunities and expand the use of technology in cybersecurity education. A more productive learning environment can also be produced by expanding access to digital resources and modernizing educational facilities.

Additionally, these educational opportunities raised students' level of awareness of safeguarding personal data and encouraged responsible behavior. Group exercises, discussions of real cyber incidents, and the use of multimedia resources all promoted active engagement while enhancing communication and critical thinking. When taken as a whole, these results show that effective cybersecurity education should foster not only technical skills but also ethical digital behavior and the self-assurance to address cybersecurity problems in every practical situation.

- *Implication for Future Research*

This research study was limited to a small sample of respondents from two universities, despite offering insights into cybersecurity teaching methods and the experiences of criminology students and graduates. To gain a more comprehensive view and improve the transferability of the findings, future studies might involve participants from different academic programs, institutions, and geographic areas. Future studies may also examine how well specific teaching techniques, such as lab exercises, simulations, and technology-based instruction, can improve students' understanding of Cybersecurity. These studies can provide further evidence in support of ongoing enhancements to cybersecurity instruction in criminology programs. Additionally, to give students practical exposure to real-world scenarios and experience, institutions may consider implementing laboratory exercises or creating a dedicated laboratory subject focused on cybersecurity-related principles. Examining how students' learning outcomes are impacted by access to digital resources, lab facilities, and tools is necessary.

Future researchers should examine the long-term effects of cybersecurity education on students, particularly for those who plan to work in law enforcement's digital forensics and cybercrime units. Additionally, comparative studies between educational institutions focus mostly on the classroom. In addition to determining how laboratory learning affects students' practical skills and career readiness, such research can help identify best practices in cybersecurity education.

V. CONCLUDING REMARKS

This study investigated the experiences of criminology students with cybersecurity education and the teaching strategies that facilitate their learning. This study investigated the experiences of criminology students with cybersecurity education and the teaching strategies that facilitate their learning. The study shows that improving students' theoretical knowledge is not the only aspect of meaningful cybersecurity education. The study demonstrates that students truly learn Cybersecurity when they can apply what they have learned. Students learn the fundamentals in the classroom, but they become more adept at problem-solving and investigation when they participate in practical activities, collaborate with others, and complete exercises that teach them by doing. These encounters give Cybersecurity greater significance and make it simpler to apply in daily life. According to the study, it is crucial to teach criminology students practical skills to address cybercrime, in addition to theory. Students should have the opportunity to participate in cybersecurity education and apply what they learn to real-world situations. In this manner, aspiring law enforcement officers will possess the competence and self-assurance necessary to carry out their duties. The secret to preparing students for the difficulties posed by cybercrime is cybersecurity education. By providing them with practical cybersecurity training, they will be better prepared for this industry.

The study also identified a few issues. One of these issues is the difficulty of comprehending cybersecurity concepts. An additional issue is the scarcity of digital tools, resources, and laboratory experiences. These issues make it difficult for students to advance their abilities. Despite students being more aware of Cybersecurity, this is still true. They grasp the ideas.

Thus, the study underscores the need for a comprehensive approach to cybersecurity education that incorporates theoretical instruction, real-world learning experiences, and appropriate technological resources for effective Cybersecurity. Providing students with experiential learning opportunities is crucial for enhancing their practical skills and cybersecurity knowledge. This calls for sufficient access to educational materials, suitable technology, and teaching strategies that actively involve students in the learning process. These experiences enhance students' capacity to apply cybersecurity techniques in real-world scenarios. Educational institutions can better prepare criminology students to tackle cybersecurity issues and help prevent cybercrime by supporting these learning matters. giving aspiring law enforcement officers the abilities, information, and real-world experience, they need to meet the demands of a society increasingly digital.

REFERENCES

[1.] Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). *Cybersecurity awareness and education programs: A review of employee engagement and accountability*. Computer Science&IT Research Journal, 5(1), 100–119.

[2.] Agbakhamen, C. O. (2025). *Ethical standards in research: A professional imperative.* Zenodo. https://doi.org/10.5281/zenodo.14875237

[3.] Ahmed, A., Watterson, C., Alhashmi, S., & Gaber, T. (2024). *How universities teach cybersecurity courses*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

online: A systematic literature review. Frontiers in Computer Science, 6, 1499490. https://doi.org/10.3389/fcomp.2024.1499490

[4.] Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). *Cyber-threat intelligence for security decision-making: A review and research agenda for practice*. Computers&Security, 132, 103352. https://doi.org/10.1016/j.cose.2023.103352

[5.] Aithal, S., & Aithal, S. (2023). *Use of AI-based GPTs in experimental, empirical, and exploratory research methods.* International Journal of Case Studies in Business, IT and Education. https://doi.org/10.47992/IJCSBE.2581.6942.0308

[6.] Alabab, B. L., Jr., Cubol, J. S., Pascual, M. A. C., Ubaldo, E. S., Sario, D. R. D., & Velasco, M. S. (2023). *Cybersecurity awareness of college students in a private higher education institution.* CGCI International Journal of Administration, Management, Education and Technology, 1(1), 51.

[7.] Alnajim, A. M., Habib, S., Islam, M., AlRawashdeh, H. S., & Wasim, M. (2023). *Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches.* Symmetry, 15(12), 2175. https://doi.org/10.3390/sym15122175

[8.] Alotaibi, F. G., Clarke, N., & Furnell, S. M. (2021). *A novel approach for improving information security management and awareness for home environments.* Information and Computer Security, 29(1), 25–48.

[9.] Alshaikh, M. (2020). *Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

[10.] Alsaeed, H. R., Elsayad, W. A., Abo Bakr, R. T. A. E. G., & Hassan, M. A. (2023). *Awareness of cybercrime risks and their relationship to attitude toward internet use among university students.* Journal of Positive Psychology and Wellbeing, 7(10), 59–76.

[11.] Altarawneh, M. H. M., Althunibat, A., Almajali, M. H., Alzriqat, N., & Alazzam, S. (2025). *Cybersecurity awareness among school students: Exploring influencing factors, legal implications, and knowledge gaps.* International Journal of Innovative Research and Scientific Studies, 8(1), 1516–1529. https://doi.org/10.53894/ijirss.v8i1.4696

[12.] Alzahrani, L. (2021). *Statistical analysis of cybersecurity awareness issues in higher education institutes.* International Journal of Advanced Computer Science and Applications, 12(11). https://doi.org/10.14569/IJACSA.2021.0121172

[13.] Angafor, G. N., Yevsereyeva, I., & He, Y. (2022). *Bridging the cyber security skills gap: Using tabletop exercises to solve the CSS crisis.* In M. Ma, B. Fletcher, S. Göbel, B. Hauge, & T. Marsh (Eds.), Serious games: JCSG 2020 (Vol. 12434, Lecture Notes in Computer Science). Springer.

[14.] Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). *A structural equation modeling approach topreservice teachers' perspectives ooncybersecurity education.* Education and Information Technologies, 29(3), 3699–3727. https://doi.org/10.1007/s10639-023-11973-5

[15.] Bada, M., & Nurse, J. R. C. (2020). *Developing cybersecurity education and awareness programs for small- and medium-sized enterprises (SMEs).* Information and Computer Security, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

[16.] Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall.

[17.] Bandura, A. (1997). *Self-efficacy: The exercise of control.* W. H. Freeman.

[18.] Blažič, A. J., & Blažič, B. J. (2024). *Teaching and learning cybersecurity for European youth by applying interactive technology and smart education.* Education and Information Technologies. Advance online publication.

[19.] Burns, M., Johnson, N. V., Grasman, K., Habibi, S. Z., Kayler, A. S., Kaehr, A., Lacar, M. F., & Yan, B. (2023). *Pedagogically grounded techniques and technologies for enhancing student learning.* Advances in Engineering Education, 11(3), 77–107.

[20.] Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). *Purposive sampling: Complex or simple? Research case examples.* Journal of Research in Nursing, 25(8), 652–661. https://doi.org/10.1177/1744987120927206

[21.] Catal C., Ozcan A., Donmez E., Kasif A. (2023). A*nalysis of cybersecurity knowledge gaps based on the cybersecurity body of knowledge.* Education and Information Technologies, 28, 1809-1831. Crossref. PubMed. Web of Science.

[22.] Churi, P., & Rao, N. T. (2021). *Teaching a cybersecurity course in the classrooms of NMIMS University.* International Journal of Modern Education and Computer Science, 13(4), 1–15. https://doi.org/10.5815/IJMECS.2021.04.01

[23.] Concoles, C. R., Cristobal, N., Felonia, E., Tadtad, V. M., Villafuerte, K. A., & Lucas, T. V. D. (2022). *Cybercrime awareness and cybercrime-prevention attitudes among criminology students.* Central Mindanao Colleges.

[24.] Cybersec4Europe Competence Center. (2022). *Enablers and components report.* https://cybersec4europe.eu/wp-content/uploads/2022/02/D3.13Updated-version-of-enablers-and-components-v3.0-submitted.pdf

[25.] Dawson, K., Antonenko, P., Xu, Z., & Wusylko, C. (2022). *Promoting interdisciplinary integration of cybersecurity knowledge, skills, and career awareness in preservice teacher education.* Journal of Technology and Teacher Education, 30(2), 275–287.

[26.] Duchatelet, D., Jossberger, H., & Rausch, A. (2022). *Assessment and evaluation of simulation-based learning in higher education and professional training: An introduction.* Studies in Educational Evaluation, 75, 101210. https://doi.org/10.1016/j.stueduc.2022.101210

[27.] Dahlan, M. M., Halim, N. S. A., Kamarudin, N. S., & Ahmad, F. S. Z. (2023). *Exploring interactive video learning: Techniques, applications, and pedagogical insights.* International Journal of Advanced and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

Applied Sciences, 10(12), 220–230. https://doi.org/10.21833/ijaas.2023.12.024

[28.] Fouché, C. B., Strydom, H., & Roestenburg, W. J. H. (2021). *Research at grassroots: For the social sciences and human service professions (5th ed.)*. Van Schaik.

[29.] Hobbs, J. (2023). *Cybersecurity awareness in higher education: A comparative analysis of faculty and staff*. Doctoral dissertation, Middle Georgia State University.

[30.] Ghazali, N., Suryani, I., & Idrus, S. Z. S. (2024). *Challenges and opportunities of cybersecurity education for non-technical majors.* Journal of Communication in Scientific Inquiry, 6(1), 47–55.

[31.] Kalukar, V. J., Krobo, A., Pessireron, M. F., Suhendra, S., & Yudistira, S. (2024). *Enhancing critical thinking skills through collaborative learning in modern educational practices.* The Journal of Academic Science, 1(8), 1145–1153. https://doi.org/10.59613/2dx5zr09

[32.] Kapur, R. (2020). *Lecture method: The most comprehensively used pedagogical method.* https://www.researchgate.net/publication/345893936_Lecture_Method_The_Compre hensively_used_Pedagogical_Method

[33.] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). *Artificial intelligence for Cybersecurity: Literature review and future research directions.* Information Fusion, 97, 101804. https://doi.org/10.1016/j.inffus.2023.101804

[34.] Kashyap, A. K., Priyanka, & Gupta, P. (2025). *Do cyber fraud experiences matter? Revisiting user motivations and satisfaction in driving FinTech continuance.* Computers&Security. https://doi.org/10.1016/j.cose.2025.104188

[35.] Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). *Enhancing employees' information security awareness in private and public organizations: A systematic literature review.* Computers & Security, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

[36.] Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development.* Prentice-Hall.

[37.] Kurt, S.,& Kurt, S. (2024, November 13). *Mayer's principles of multimedia learning.* Educational Technology. https://educationaltechnology.net/mayers-principles-of-multimedia-learning/

[38.] Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation.* Cambridge University Press.

[39.] Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., & Fujdiak, R. (2025). *Lessons learned from using a cyber range to teach Cybersecurity at different levels of education.* Technology, Knowledge, and Learning. https://doi.org/10.1007/s10758-025-09840-y

[40.] Marougkas, A., Troussas, C., Krouska, A., & Sgouropoulou, C. (2023). *Virtual reality in education: A review of learning theories, approaches, and methodologies for the last decade.* Electronics, 12(13), 2832. https://doi.org/10.3390/electronics12132832

[41.] McLeod, S. (2025, March 19). *Kolb's learning styles & experiential learning cycle. Simply Psychology.* https://www.simplypsychology.org/learning-kolb.html

[42.] Mukherjee, M., Le, N. T., Chow, Y., & Susilo, W. (2024). *Strategic approaches to cybersecurity learning: A study of educational models and outcomes.* Information, 15(2), 117. https://doi.org/10.3390/info15020117

[43.] Morrow, E. (2024). *Scamming higher ed: An analysis of phishing content and trends.* Computers in Human Behavior, 158, 108274.

[44.] Nasir, S. N. S. (2023). *Exploring the effectiveness of cybersecurity training programs: Factors, best practices, and future directions.* Advances in Multidisciplinary&Scientific Research Journal Publication, 2(1), 151–160. https://doi.org/10.22624/aims/csean-smart2023p18

[45.] Netwrix (2023). *3 out of 4 cyberattacks in the education sector are associated with a compromised on-premises user or admin account.* https://netwrix.com/en/resources/news/3-of-4-education-cyberattacks-associated-with-compromised-on-prem-accounts/

[46.] Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2024). *Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis.* Computers & Security, 150, 104276. https://doi.org/10.1016/j.cose.2024.104276

[47.] Osborne, N., & Grant-Smith, D. (2021). *In-depth interviewing. In S. Baum (Ed.), Methods in urban analysis (Cities Research Series).* Springer. https://doi.org/10.1007/978-981-16-1677-8_7

[48.] Prümmer, J., Van Steen, T., & Van Den Berg, B. (2023). *A systematic review of current cybersecurity training methods.* Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

[49.] Raffaghelli, J. E., Rodríguez, M. E., Guerrero-Roldán, A., & Bañeres, D. (2022). *Applying the UTAUT model to explain the students' acceptance of an early warning system in Higher Education.* Computers & Education, 182, 104468. https://doi.org/10.1016/j.compedu.2022.104468

[50.] Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). *Semi-structured interview: A methodological reflection on the development of a qualitative research instrument in educational studies.* IOSR Journal of Research & Method in Education, 12(1), 22–29.

[51.] Sarita, K., Kaur, K., Kaur, P., & Kaur, S. (2024). *Review of learning strategies for cybersecurity awareness among students in the online teaching era.* Zenodo. https://doi.org/10.5281/zenodo.10949000

[52.] Schumacher, C., & Ifenthaler, D. (2020). *Investigating prompts for supporting students' self-regulation—A remaining challenge for learning analytics approaches?* The Internet and Higher Education, 49, 100791. https://doi.org/10.1016/j.iheduc.2020.100791

[53.] Silitubun, E., Mustaji, M., & Dewi, U. (2025). *The*

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26sep056

effectiveness of case-based learning in enhancing students' critical thinking skills. Journal of Neonatal Surgery, 14(2), 136–141. https://doi.org/10.52783/jns.v14.1844

[54.] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & Von Solms, B. (2022). *Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise.* Computers & Security, 119, 102756. https://doi.org/10.1016/j.cose.2022.102756

[55.] Shivapurkar, M., Bhatia, S., & Ahmed, I. (2020). *Problem-based learning for cybersecurity education.* Journal of the Colloquium for Information Systems Security Education, 7(1). https://doi.org/10.53735/cisse.v7i1.108

[56.] Thomas, F. B. (2022). *The role of purposive sampling as a tool for informal choice in research methods in the social sciences.* Just Agriculture, 2(5), 1–8.

[57.] Yang, S. C. (2021). *A meta-model of cybersecurity curricula: Assessing cybersecurity curricular frameworks for business schools.* Journal of Education for Business, 96(2), 99–110. https://doi.org/10.1080/08832323.2020.1757594

[58.] Vaish, A., Kumar, R., Bobek, S., & Sternad, S. (2024). *Development of a cybersecurity platform for experiential learning.* Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 22. https://doi.org/10.62915/2472-2707.1184

[59.] Vanover, C. (2022). Transcription is a form of qualitative inquiry. *Analyzing and interpreting qualitative research: After the interviewer*, 63–79.

[60.] Zafar, H., Hollingsworth, C. L., Bandyopadhyay, T., & Randolph, A. B. (2024). *Collaborative Pathways to Cybersecurity Excellence: Insights from Industry and Academia in the Southeastern US*. Journal of Cybersecurity Education, Research and Practice, 2024(1).

[61.] Zajda, J. (2021). *Constructivist learning theory and creating effective learning environments*. In Globalization, comparative education and policy research (pp. 35–50). Springer. https://doi.org/10.1007/978-3-030-71575-5_3.

[62.] Zwilling M., Klien G., Lesjak D., Wiechetek Cetin F, Basim H. N. (2022). *Cyber security awareness, knowledge, and behavior: A comparative study.* Journal of Computer Information Systems, 62(1), 82–9.