Cyber-Threat Scenario Realism in Digital Simulation: Effects on Educational Technology Students' Threat Detection and Digital Incident Response Skills

Mohamed W. Soliman[1], Mahmoud N. Rashwan[2], Tamer M. Kamel[3]

[1] Faculty of Specific Education, Alexandria University, Alexandria, Egypt;
mohamed_wahid2007@alexu.edu.eg
[2] Faculty of Specific Education, Ain Shams University, Cairo, Egypt;
dr.mahmoud.nasr@sedu.asu.edu.eg
[3] Faculty of Specific Education, Kafr Elsheikh University, Kafr Elsheikh, Egypt;
Dr_Tamerkamel@spe.kfs.edu.eg

Abstract

This study examined the effect of cyber-threat scenario realism, high-realism versus low-realism, within a digital simulation environment on Educational Technology students' threat detection and digital incident response skills. A quasi-experimental pretest–posttest design with two experimental groups was used. The sample consisted of 100 second-level Educational Technology students, with 50 students assigned to each group. The high-realism group learned through cyber-threat scenarios that included multiple evidence sources, appropriate ambiguity, incident progression, and decision consequences, whereas the low-realism group learned through simpler and more direct scenarios addressing the same skills. The instruments included a core concepts test, two situational tests, two performance rubrics, an interaction analysis log, and a perceived scenario realism scale. Data were analyzed using means, standard deviations, independent-samples t-tests, ANCOVA, gain scores, and effect sizes. The results showed statistically significant posttest differences in favor of the high-realism group across all instruments. The strongest effects appeared in the performance rubrics and interaction analysis log, indicating that high-realism scenarios were particularly effective in developing applied and behavioral dimensions of detection and response. The findings suggest that scenario realism is a meaningful instructional design variable in educational cybersecurity simulation and can help Educational Technology students move from general awareness toward evidence-based and procedurally safe digital incident response.

Keywords: scenario realism; cyber-threat scenarios; digital simulation; threat detection; digital incident response; educational technology.

Introduction

Digital learning environments have undergone a profound transformation in recent years. Learning management systems, institutional email, cloud storage, virtual meeting platforms, file-sharing systems, and digital collaboration tools are no longer peripheral supports for teaching and learning. They have become operational infrastructures through which students, teachers, and educational institutions manage learning processes, exchange data, organize activities, store records, and sustain academic communication.

With this increasing dependence on digital environments, cybersecurity risks have become part of everyday educational practice. These risks may appear in the form of phishing messages, fraudulent links, suspicious files, compromised accounts, unsafe file-sharing permissions, or unintended disclosure of educational data. The Cybersecurity Framework issued by the National Institute of Standards and Technology emphasizes that cybersecurity risk management requires a set of interrelated functions, including identify, protect, detect, respond, and recover. Within this framework, threat detection and incident response represent essential components of safe digital practice in educational institutions (National Institute of Standards and Technology [NIST], 2018).

This issue is particularly significant in the field of Educational Technology. Educational Technology students do not engage with digital tools merely as ordinary users. Rather, they are being prepared for professional roles that involve designing digital content, managing learning environments, supporting teachers and learners, organizing electronic learning resources, and employing web-based and cloud-based tools in a wide range of instructional contexts. Accordingly, a limited ability to detect a digital threat or respond safely to a simple incident may later affect entire learning environments that these students design, manage, or support.

From this perspective, preparing Educational Technology students cannot be considered complete if it focuses only on design, production, and technology use while neglecting the basic defensive skills required for safe participation in digital learning environments. The NICE Cybersecurity Workforce Framework supports this view by representing cybersecurity work as a set of tasks, knowledge areas, and skills that can be described, taught, and assessed. This makes it possible to translate selected cybersecurity competencies into educationally appropriate learning outcomes for students who are not specialists in advanced cybersecurity (Petersen et al., 2020).

Recent studies have also shown that many digital threats targeting users exploit human behavior before they exploit technical vulnerabilities. Phishing, social engineering, and unsafe sharing practices do not always depend on technical sophistication. Instead, they often rely on persuading users to make quick, unsafe decisions. General awareness or abstract advice is therefore insufficient for developing secure digital behavior. A student may know that phishing is dangerous, yet fail to detect a phishing message when

it resembles an official communication or appears within a familiar educational context. Effective cybersecurity training should therefore move beyond direct instruction and place learners in situations that require them to identify indicators, analyze risk, and make appropriate decisions, so that knowledge becomes observable behavior (Egelman & Peer, 2015). Digital simulation environments offer a suitable approach for developing this type of skill. They allow potentially risky or suspicious situations to be represented in a safe educational setting, where students can inspect evidence, compare indicators, make decisions, and receive feedback without exposing real systems, accounts, or educational data to harm. Reviews of simulation-based learning in higher education indicate that simulations are more effective when they engage learners in active situations requiring performance and decision-making rather than merely presenting information or procedures in a static form (Chernikova et al., 2020). Similarly, research on games and simulations in higher education suggests that the effectiveness of such environments depends on the design of the activity, the clarity of objectives, the nature of interaction, and the extent to which the task is meaningfully connected to the learner's context (Vlachopoulos & Makri, 2017).

The value of simulation, however, does not emerge simply from using a digital platform or interactive activity. It is shaped by the nature of the scenario that the environment presents. A low-realism scenario may present a threat in an obvious and direct form, such as a message that explicitly asks for a password or a link that is described in advance as unsafe. In such cases, the learner may treat the situation as a simple recognition exercise. By contrast, a high-realism scenario places the learner in a situation that more closely resembles authentic digital practice. It may include multiple pieces of evidence, gradually emerging warning signs, a degree of uncertainty, and consequences attached to the learner's decision. Cybersecurity training literature emphasizes that a scenario is not merely a narrative frame or a background story; it is a structural component that defines the event, the trainee's behavior, the required decision, the assessment indicators, and the feedback pathway (Yamin et al., 2020).

Accordingly, the present study does not examine digital simulation as a general instructional medium. Instead, it focuses on the realism level of cyber-threat scenarios as an independent instructional design variable. The central question is not whether simulation supports learning, but whether increasing the realism of scenarios within the same simulation environment leads to greater development of cyber-threat detection and digital incident response skills compared with less realistic scenarios, while holding the platform, content, time, and assessment tools constant.

This question is important because scenario design in simulation environments often falls between two problematic extremes. Excessive simplification may produce scenarios that do not resemble real practice, whereas excessive complexity may overwhelm learners and reduce the educational value of the experience. The present study therefore examines high realism as structured instructional realism, not as an uncontrolled accumulation of details.

The study consequently developed a safe digital simulation environment based on two levels of cyber-threat scenario realism. It then examined the effects of these two levels on students' core concepts, cyber-threat detection skills, practical threat detection performance, digital incident response skills, practical response performance, and interaction quality within the environment. The study also measured students' perceived realism of the scenarios to verify that the experimental manipulation was meaningful from the learners' perspective.

To clarify the conceptual logic of the study, Figure 1 presents the relationship between the independent variable, cyber-threat scenario realism level, and the digital simulation environment as the context in which the treatment was implemented. It also shows the dependent variables, namely cyber-threat detection skills, digital incident response skills, and interaction quality within the simulation environment. Perceived scenario realism was included as a manipulation check rather than as a primary dependent variable.

Figure 1 Conceptual Model of the Study

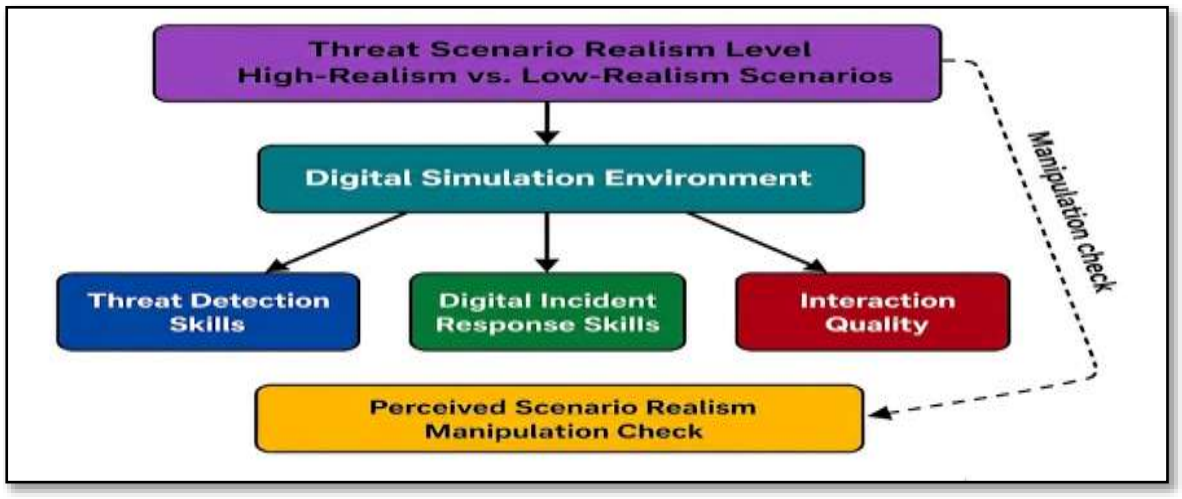


Figure 1 shows that cyber-threat scenario realism is not treated as a superficial feature of the learning environment. Rather, it is conceptualized as an instructional design variable that shapes the nature of the learning experience students undergo within the simulation. High-realism scenarios are expected to expose students to digital situations that are closer to those encountered in real learning environments. Such scenarios include multiple forms of evidence, appropriate ambiguity, a logical sequence of incident development, and consequences for decisions. These features are expected to improve the quality of detection, response, and interaction within the simulation environment.

Research Problem

The problem addressed in the present study emerges from the mismatch between the nature of Educational Technology students' future roles in digital learning environments and the limited structured preparation they receive in cyber-threat detection and digital incident response. Educational Technology students routinely engage with learning management systems, institutional email, shared files, educational links, login records, student data, and digital communication tools. All of these components may become vulnerable points if users lack adequate security awareness and basic defensive performance skills.

The review of the Educational Technology program regulations indicated that the program did not include a separate course or a structured instructional unit addressing educational cybersecurity, cyber-threat detection, or digital incident response procedures. As a result, students' knowledge of these issues tended to be general, fragmented, and unsupported by intentional academic training.

This problem was not merely theoretical. It also appeared in an exploratory field experience conducted with a group of second-level Educational Technology students. The exploratory results showed that many students were unable to distinguish accurately between official messages and phishing messages. Some students treated untrusted links as ordinary links when they appeared within a familiar educational context. Others showed weaknesses in basic response procedures, such as preserving evidence, documenting an incident, escalating it to the appropriate authority, and avoiding the redistribution of a suspicious link or the opening of a questionable file.

The issue therefore extends beyond a lack of theoretical knowledge. Some students may be able to define a digital threat in general terms, yet fail to detect it when it appears in a realistic educational situation. This gap is particularly important because cybersecurity literature increasingly emphasizes that non-specialist users need situated training that supports secure decision-making at the moment of interaction with risk. Social engineering, phishing, and unsafe permission settings often exploit weaknesses in attention, judgment, and decision-making. Effective training should therefore place learners in situations close to real digital use, where they learn how to inspect evidence before acting, weigh possibilities, and avoid actions that may increase harm (Aldawood & Skinner, 2018).

Although digital simulation appears to be an appropriate approach for training students in these skills, the core issue is not the use of simulation in itself. Rather, it concerns the realism level of the scenarios embedded within the simulation environment. A low-realism scenario may help students learn an obvious indicator, but it may not adequately prepare them for more ambiguous situations that resemble actual digital practice, where evidence is not always direct and the correct response is not immediately apparent. A high-realism scenario, by contrast, may support deeper performance-based learning because it approximates the structure of real digital incidents through multiple indicators, ambiguity, gradual information disclosure, and consequences attached to the learner's decision. Reviews of cybersecurity training environments indicate that scenario design is one of the most important components of training because it determines the required performance, success indicators, and interaction pathway between the trainee and the simulated situation (Kavak et al., 2021).

Accordingly, the problem of the present study can be stated as follows: Educational Technology students show weaknesses in cyber-threat detection and digital incident response skills, and there is a need to examine whether the realism level of cyber-threat scenarios within a digital simulation environment affects the development of these skills. More specifically, the study investigates whether high-realism scenarios lead to greater improvement than low-realism scenarios.

The main research question was therefore formulated as follows:

What is the effect of cyber-threat scenario realism level, high-realism versus low-realism, within a digital simulation environment on developing cyber-threat detection and digital incident response skills among Educational Technology students?

Research Questions

The main research question was addressed through the following sub-questions:

1. What cyber-threat detection and digital incident response skills are required for Educational Technology students?
2. What design standards are needed for developing a digital simulation environment based on high-realism and low-realism cyber-threat scenarios?
3. What is the structure of the experimental treatment based on high-realism cyber-threat scenarios within the digital simulation environment?
4. What is the structure of the experimental treatment based on low-realism cyber-threat scenarios within the digital simulation environment?
5. What is the effect of cyber-threat scenario realism level on developing students' core

concepts related to cyber-threat detection and digital incident response?
6. What is the effect of cyber-threat scenario realism level on developing students' cyber-threat detection skills?
7. What is the effect of cyber-threat scenario realism level on developing students' practical cyber-threat detection performance within the digital simulation environment?
8. What is the effect of cyber-threat scenario realism level on developing students' digital incident response skills?
9. What is the effect of cyber-threat scenario realism level on developing students' practical digital incident response performance within the digital simulation environment?
10. What is the effect of cyber-threat scenario realism level on the quality of students' interaction within the digital simulation environment?
11. Do students in the high-realism scenario group perceive the scenarios they experienced as more realistic than those experienced by students in the low-realism scenario group?

Research Hypotheses

In light of the research problem, research questions, nature of the experimental treatment, and literature on digital simulation and cybersecurity training, the following hypotheses were formulated:

1. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the test of core concepts related to cyber-threat detection and digital incident response, in favor of the high-realism scenario group.
2. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the cyber-threat detection situational test, in favor of the high-realism scenario group.
3. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the performance observation rubric for cyber-threat detection within the digital simulation environment, in favor of the high-realism scenario group.
4. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the digital incident response situational test, in favor of the high-realism scenario group.
5. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the digital incident response performance assessment rubric within the digital simulation environment, in favor of the high-realism scenario group.
6. There is a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the interaction analysis log within the digital simulation environment, in favor of the high-realism scenario group.
7. There is a statistically significant difference at the .05 level between the mean scores of students in the two experimental groups on the perceived cyber-threat scenario realism scale, in favor of the high-realism scenario group.
8. The high-realism scenario group achieves greater gain than the low-realism scenario group across the research instruments measuring cyber-threat detection and digital incident response.

Research Objectives

The main objective of the present study was to examine the effect of cyber-threat scenario realism level, high-realism versus low-realism, within a digital simulation environment on developing cyber-threat detection and digital incident response skills among Educational Technology students.

This main objective was addressed through the following specific objectives:

1. To identify the cyber-threat detection and digital incident response skills required for Educational Technology students.
2. To develop a list of design standards for a digital simulation environment based on high-realism and low-realism cyber-threat scenarios.
3. To design a safe educational digital simulation environment that presents cyber-threat scenarios within familiar educational contexts.
4. To design high-realism cyber-threat scenarios that include multiple pieces of evidence, appropriate ambiguity, incident progression, and consequences for decisions.
5. To design low-realism cyber-threat scenarios that address the same skills in a simpler and more direct form.
6. To measure the effect of scenario realism level on developing students' core concepts related to cyber-threat detection and digital incident response.
7. To measure the effect of scenario realism level on developing students' cyber-threat detection skills.
8. To measure the effect of scenario realism level on developing students' practical cyber-threat detection performance within the digital simulation environment.
9. To measure the effect of scenario realism level on developing students' digital incident response skills.
10. To measure the effect of scenario realism level on developing students' practical digital

incident response performance within the simulation environment.

11. To analyze the quality of students' interaction within the digital simulation environment in terms of evidence inspection, detection accuracy, response quality, performance efficiency, independence, safe behavior, and documentation.
12. To verify the validity of the experimental manipulation by measuring students' perceived realism of the scenarios they experienced.

Significance of the Study

Theoretical Significance

The theoretical significance of the present study lies in its focus on a topic that connects Educational Technology with educational cybersecurity, a field whose importance has increased as learning environments have become data-driven, account-based, permission-sensitive, and continuously interactive digital systems. Cybersecurity risk in educational environments is not limited to technical infrastructure. It is also shaped by user behavior, the ability to recognize risk indicators, and the capacity to act safely.

The study therefore contributes to broadening the concept of preparing Educational Technology students. Such preparation should not be restricted to design, production, and digital environment management. It should also include basic defensive skills that help protect digital learning environments and support safer educational practice.

The study also contributes theoretically by treating scenario realism as an instructional design variable within digital simulation environments. Many studies approach simulation as a single instructional medium. The present study, however, distinguishes between high-realism and low-realism scenarios while controlling the remaining components of the learning environment. This distinction allows a more precise understanding of how scenario characteristics influence the learning of practical cybersecurity-related skills.

In addition, the study enriches the measurement of educational cybersecurity skills among non-specialist learners. It does not rely solely on a knowledge test. Instead, it uses situational tests, performance rubrics, an interaction analysis log, and a perceived realism scale. This integrated measurement approach makes it possible to examine the educational effect from multiple perspectives: knowledge, decision-making, practical performance, behavior within the environment, and the learner's perception of the experimental treatment.

Practical Significance

The practical significance of the study lies in the fact that it provides a developable model for a safe digital simulation environment that can help Educational Technology programs integrate educational cybersecurity skills into students' academic preparation. This model is not intended to prepare cybersecurity specialists or train students in offensive practices. Rather, it focuses on defensive skills appropriate to the nature of Educational Technology students' future roles, such as inspecting messages and links, reviewing file permissions, analyzing activity logs, documenting incidents, and escalating problems safely.

The findings may also benefit faculty members and course designers who wish to develop short instructional units on educational cybersecurity within courses related to learning management systems, digital learning environment design, e-learning, digital learning resources, and field training. The value of such units lies in presenting cybersecurity through familiar educational situations rather than isolating it within an abstract technical context. This direction is consistent with contemporary approaches to problem-based and scenario-based learning, in which learners acquire knowledge through meaningful real-world problems rather than through decontextualized information.

The research instruments may also be useful for educational institutions and researchers interested in measuring multiple dimensions of educational cybersecurity skills. The core concepts test measures supporting knowledge; the situational tests measure decision quality; the performance rubrics measure practical execution; the interaction log reveals the process of performance; and the perceived realism scale verifies the experimental manipulation.

Delimitations of the Study

Subject Delimitations

The present study was delimited to examining the effect of cyber-threat scenario realism level, high-realism versus low-realism, within a digital simulation environment on developing cyber-threat detection and digital incident response skills among Educational Technology students.

The instructional content focused on threats associated with digital learning environments, including phishing messages, suspicious links, impersonation, credential theft, suspicious files, unusual account activity, data leakage, unsafe file-sharing permissions, evidence preservation, documentation, escalation, and secure communication.

Human Delimitations

The main study sample consisted of 100 second-level students enrolled in the Department of Educational Technology. They were assigned to two equivalent experimental groups: 50 students in the high-realism scenario group and 50 students in the low-realism scenario group.

The study also used a pilot sample of 20 students who were not included in the main sample. This pilot group was used to verify the clarity of the instruments and the simulation environment and to calculate reliability indicators. In addition, an exploratory sample of 50 students was used to diagnose the field manifestations of the research problem.

Temporal Delimitations

The study was implemented during the first semester of the 2022/2023 academic year. Both groups followed a unified implementation plan and were exposed to the same content, activities, and tasks during the same period. The only systematic difference between the groups was the realism level of the cyber-threat scenarios.

Spatial Delimitations

The study was conducted at the Faculty of Specific Education, with students from the Department of Educational Technology, within a university learning context that uses digital learning environments and electronic interaction tools familiar to the students.

Instrumental Delimitations

The study was delimited to the following research instruments: the test of core concepts related to cyber-threat detection and digital incident response, the cyber-threat detection situational test, the performance observation rubric for cyber-threat detection within the digital simulation environment, the digital incident response situational test, the digital incident response performance assessment rubric within the digital simulation environment, the interaction analysis log within the digital simulation environment, and the perceived cyber-threat scenario realism scale.

Technological Delimitations

The study was delimited to a safe educational digital simulation environment. Moodle was used as the operational platform for organizing and delivering the treatment, supported by interactive activities, documentation forms, and guided interaction records.

The environment was not a specialized cyber range, nor was it designed to train cybersecurity experts. It did not include malicious links, infected files, harmful code, or offensive cybersecurity practices. All evidence, files, accounts, and logs used in the scenarios were simulated and safe.

Operational Definitions of Key Terms

Cyber-Threat Scenario Realism Level

Cyber-threat scenario realism level is operationally defined in the present study as the degree to which a threat scenario presented within the digital simulation environment approximates possible digital educational situations in real practice. This realism is reflected in the context in which the threat appears, the nature of evidence and indicators, the sequence of incident development, the degree of ambiguity, time pressure, decision consequences, and the tools used for inspection, documentation, and response.

In the present study, this variable was represented by two experimental levels: high-realism scenarios and low-realism scenarios.

High-Realism Cyber-Threat Scenarios

High-realism cyber-threat scenarios are operationally defined as educational digital simulation situations that present cyber threats within contexts close to actual digital learning environments, such as the learning platform, institutional email, cloud storage, virtual meetings, and activity logs.

These scenarios include multiple and distributed pieces of evidence, appropriate ambiguity, a logical incident sequence, moderate time pressure, and consequences linked to the student's decision. They require the student to inspect evidence, analyze indicators, estimate risk, and document the decision before selecting a response.

Low-Realism Cyber-Threat Scenarios

Low-realism cyber-threat scenarios are operationally defined as educational digital simulation situations that present the same cyber threats addressed in the high-realism scenarios, but in a simpler and more direct form.

In these scenarios, evidence is fewer in number, warning indicators are more explicit, ambiguity is limited, the incident sequence is shorter, and decision consequences are less detailed. The situation is therefore closer to direct training on a concept or procedure.

Digital Simulation Environment

The digital simulation environment is operationally defined as a safe Moodle-based electronic learning environment designed to present interactive cyber-threat scenarios for Educational Technology students. It includes instructional content, interactive activities, simulated digital evidence, decision pathways, documentation forms, and interaction records.

The purpose of the environment is to train students in cyber-threat detection and digital incident response. It is not a specialized cybersecurity laboratory or an offensive training environment. It is a safe defensive educational simulation that contains no harmful links, infected files, or risky practices.

Cyber-Threat Detection Skills

Cyber-threat detection skills are operationally defined as the cognitive and practical performances that enable Educational Technology students to inspect the elements of a digital situation, collect evidence, analyze suspicious indicators, identify the type of threat, estimate its severity, distinguish between a genuine threat and a false alarm, and document a justified detection decision within the digital simulation environment.

These skills were measured using the cyber-threat detection situational test, the performance observation rubric for cyber-threat detection, and the interaction analysis log.

Digital Incident Response Skills

Digital incident response skills are operationally defined as the safe and organized procedures performed by Educational Technology students when they detect or suspect a digital incident within a digital learning environment. These procedures include initial verification, response prioritization, containment of impact, evidence preservation, incident documentation, escalation to the appropriate authority, secure communication, initial recovery, and the

proposal of preventive action to reduce the likelihood of recurrence.

These skills were measured using the digital incident response situational test, the digital incident response performance assessment rubric, and the interaction analysis log within the digital simulation environment.

Digital Incidents

Digital incidents are operationally defined in the present study as situations in which the digital learning environment, its users, data, or resources may be exposed to a negative impact resulting from a cyber threat or unsafe digital behavior. Examples include opening a suspicious link, responding to a phishing message, exposing an educational file through public sharing permissions, ignoring an unusual login attempt, or deleting digital evidence before documenting it.

Interaction Quality within the Digital Simulation Environment

Interaction quality within the digital simulation environment is operationally defined as the level of efficiency, depth, and safety shown in students' behavior while interacting with cyber-threat scenarios. It is reflected in evidence inspection, detection accuracy, response decision quality, performance efficiency, independence, avoidance of unsafe behavior, and quality of documentation.

In the present study, interaction quality was measured using the interaction analysis log within the digital simulation environment.

Perceived Cyber-Threat Scenario Realism

Perceived cyber-threat scenario realism is operationally defined as the degree to which students judge the scenarios they experienced within the simulation environment to be close to digital educational situations that may occur in real practice. This perception includes the realism of the threat context, evidence and indicators, incident sequence, inspection and response tools, time pressure, decision consequences, and ambiguity during decision-making. It was measured using the perceived cyber-threat scenario realism scale, which was administered after the treatment as a manipulation check.

Theoretical Framework and Previous Studies Overview

The theoretical framework of the present study is grounded in the assumption that cyber-threat detection and digital incident response skills cannot be developed effectively through abstract theoretical knowledge alone. These skills are situated, evidence-based, and decision-oriented. They require learners to interpret digital cues, inspect available evidence, judge levels of risk, and act safely in situations that may involve ambiguity, time pressure, and competing possibilities.

Accordingly, the theoretical framework is organized around five interrelated themes: cybersecurity in digital learning environments, cyber-threat detection skills, digital incident response skills, digital simulation as a safe practice-based learning approach, and cyber-threat scenario realism as an influential instructional design variable within the simulation environment.

The purpose of this framework is not to provide a general overview of cybersecurity. Rather, it is to establish the theoretical basis for understanding why high-realism scenarios may be more effective than low-realism scenarios in developing cyber-threat detection and digital incident response skills among Educational Technology students.

Cybersecurity in Digital Learning Environments

The increasing digitization of higher education has reshaped the relationship among students, teachers, content, data, and platforms. A digital learning environment is no longer a simple channel for delivering instructional materials. It is a complex space that includes login accounts, shared files, performance records, access permissions, external links, communication channels, data-collection forms, and integrations with multiple cloud services.

Consequently, the security of such environments does not depend solely on technical infrastructure. It is also shaped by users' behavior and their ability to identify unusual indicators and act safely. The NIST Cybersecurity Framework emphasizes that cybersecurity risk management is not limited to preventive protection. It also includes detection, response, and recovery. These functions are closely connected to how users behave within digital systems (NIST, 2018).

Cybersecurity becomes especially important in educational contexts because the data circulated within learning environments is not neutral. It may include personal information, grades, student submissions, assessment comments, instructional materials, work files, attendance links, and academic communications. Therefore, a mistake in sharing a file, opening a suspicious link, or ignoring an unusual login attempt may have consequences that extend beyond an individual user to peers, courses, or the institution itself.

Research on information security awareness has shown that human behavior remains a central factor in information security. Weak attention, excessive trust, and poor risk judgment may make users vulnerable even when technical systems are reasonably well protected (Parsons et al., 2017). This point is particularly relevant to Educational Technology programs, where students engage with technology not only as users but also as future designers, facilitators, and supporters of digital learning environments.

For Educational Technology students, cybersecurity cannot be treated as an external or unrelated topic. These students learn how to design content, manage platforms, employ applications, analyze learners' needs, and build digital learning environments. Therefore, a functional level of cyber-threat detection and digital incident response skill should be regarded as part of their future professional competence. The NICE Framework supports this position by describing cybersecurity work through tasks, knowledge, and skills that can be identified, taught, and assessed. Such a structure allows selected defensive cybersecurity

skills to be adapted for non-cybersecurity specializations when these skills are relevant to their actual professional roles (Petersen et al., 2020).

The nature of common threats in digital learning environments further highlights the importance of this issue. A phishing attempt may appear as a message seemingly sent from a learning platform. Credential theft may occur through a fake password update link. Data leakage may result from sharing a file containing student information through a public link. Impersonation may take the form of a message from an account that resembles that of a faculty member or platform administrator. Studies of secure behavior indicate that users may make unsafe decisions when a situation appears familiar, when they feel time pressure, or when they trust the surface appearance of a message without inspecting more precise evidence (Williams et al., 2018).

For this reason, teaching cybersecurity to Educational Technology students should not take the form of advanced technical training in network analysis or penetration testing. Instead, it should be presented as defensive educational practice connected to their realistic contexts. Students need to learn how to inspect a link without opening it, notice domain inconsistencies, review file-sharing permissions, document an incident, and escalate the problem to the appropriate authority without spreading the risk. The aim is not to turn Educational Technology students into cybersecurity specialists, but to prepare them to become safer users, designers, and supporters of digital learning environments.

Cyber-Threat Detection Skills

Cyber-threat detection is the starting point of any safe digital response. If users fail to notice a risk indicator, they are unlikely to take an appropriate action. If they misinterpret the indicator, they may either overreact or ignore the incident altogether. Detection does not simply mean naming a threat. It involves reading the digital situation through available evidence: who sent the message, what type of link is included, whether the domain is legitimate, whether there is urgency or psychological pressure, whether a file is publicly accessible, whether login records show unusual activity, and whether the available evidence is sufficient for making a justified judgment.

Cyber situational awareness literature suggests that understanding a cyber situation requires collecting and interpreting multiple indicators in context, rather than relying on a single cue or immediate impression (Franke & Brynielsson, 2014). Although this work predates the primary period of the present study's more recent literature base, its logic has been extended in later cybersecurity training research focusing on scenario-based practice and observable user behavior.

In the present study, cyber-threat detection skills comprise five interrelated processes. The first is inspecting scenario elements and collecting evidence. This requires students to treat a message, link, file, or log as a source of evidence rather than as a superficial object. The second is analyzing suspicious indicators. At this stage, the student moves from noticing signs to interpreting them, such as connecting a domain mismatch with a request for credentials and urgent wording. The third process is identifying the type of threat, such as phishing, impersonation, data leakage, or unsafe access permission. The fourth is estimating threat severity, because some indicators may reflect low-level risk, whereas others may indicate potential harm to accounts or student data. The fifth process is documenting the detection decision so that the judgment is not merely an unsupported guess.

The performance observation rubric for cyber-threat detection in the present study was therefore built around these five dimensions: inspecting scenario elements and collecting evidence, analyzing suspicious indicators, identifying the threat type, estimating severity, and documenting the detection decision.

Recent literature on phishing and social engineering indicates that users' ability to detect threats is influenced by their attention to subtle cues, previous experience, and the realism of the training they receive. Effective fraudulent messages do not always appear poorly written or obviously dangerous. They may use familiar logos, domains that closely resemble legitimate ones, formal language, and requests that seem relevant to the user's context. Training that exposes learners only to highly obvious examples may therefore be insufficient for real-life digital practice. Jampen et al. (2020), in their review of anti-phishing training, found that more effective approaches are those that provide users with applied experiences or simulated situations that help them notice deceptive indicators during practice rather than only after errors occur.

This supports the position that cyber-threat detection is not merely definitional knowledge. A student may know that phishing is an attempt to deceive users into revealing credentials, yet fail to detect a phishing message when it is carefully designed and embedded in an educational context. Similarly, a student may know that data sharing can be risky, yet fail to recognize that a Google Drive file made available to "anyone with the link" is unsafe when it contains student data. For this reason, the present study treats detection as an analytical and situated performance measured through a situational test, a performance observation rubric, and an interaction log, rather than through a knowledge test alone.

Within this context, scenario realism becomes especially important. A realistic scenario gives the student an opportunity to form a judgment from multiple indicators. A direct scenario, however, may guide the student toward the correct answer without requiring genuine inspection. When students receive a message containing a slightly altered domain, a shortened link, an urgent request, and an unusual login record, they must connect pieces of evidence. This process resembles the structure of real digital situations. By contrast, when the scenario explicitly tells the learner that a link is suspicious, the student may learn the answer more than the detection skill itself.

Digital Incident Response Skills

Digital incident response skills are no less important than detection skills. Detecting a threat does not automatically mean responding to it correctly. A student may notice a threat but still make a decision that increases harm, such as opening a link to "check" it, deleting a message before documenting it, forwarding a suspicious file to colleagues as a warning, changing a password through a fake page, or avoiding escalation because the incident seems minor.

Digital incident response therefore requires an organized sequence of action after detection. The student needs to move from initial verification to containment, then to evidence preservation and documentation, escalation and secure communication, and finally initial recovery and prevention.

In the present study, digital incident response does not refer to advanced technical response performed by information security professionals. Rather, it refers to the safe initial response appropriate for Educational Technology students. Such response may include avoiding the opening of a suspicious link, preserving evidence without altering it, correcting unsafe file-sharing permissions, changing a password through an official channel rather than through a received link, informing the platform administrator or technical support, avoiding the disclosure of sensitive information while warning others, and documenting the incident in a report form.

The digital incident response performance assessment rubric in the present study was therefore designed to measure five dimensions: initial verification and response prioritization, incident containment and impact reduction, evidence preservation and practical documentation, escalation and secure communication, and initial recovery with prevention of recurrence.

Security culture literature suggests that effective training must help users convert security intention into actual behavior. Many users know, at a general level, that they should not open suspicious links or share passwords. However, they may behave differently when under pressure, in a hurry, or when they trust the apparent source of a request. McCormac et al. (2017) showed that information security awareness is shaped by cognitive, behavioral, and organizational factors, and that improving awareness requires interventions that go beyond instructions to support more stable practices.

This supports the present study's reliance on scenarios that require students to practice response within a situation rather than memorize a list of procedures. Digital incident response is also connected to educational responsibility. An Educational Technology student may not be the final authority responsible for resolving a major incident, but they may be the first person to see an indicator, receive a report, or assist another user. They therefore need to know the boundaries of their role: what to do, what not to do, when to document, when to escalate, and how to communicate without expanding the impact of the incident.

High-realism scenarios can help develop this procedural pathway because students see the consequences of their decisions inside the situation. If they delete a message before documenting it, evidence is lost. If they redistribute a suspicious link, the risk expands. If they leave a student-data file publicly accessible, the leak continues. If they escalate without documentation, the quality of the report is reduced. In this way, learning becomes tied to the consequences of decisions rather than to the selection of an answer from a list of alternatives. This explains why decision consequences were included as one of the key dimensions of scenario realism in the present study.

Digital Simulation as a Practice-Based Approach for Educational Cybersecurity Skills

Digital simulation presents a situation, system, or event in a safe instructional form that allows learners to interact, make decisions, observe consequences, and receive feedback without exposure to actual risk. For a topic such as educational cybersecurity, simulation is particularly valuable because direct training on real threats is neither ethically nor practically appropriate for Educational Technology students.

Simulation allows the design of situations such as a phishing message, an incorrectly shared file, or an unusual login record while ensuring that all links, files, accounts, and data are simulated and safe. This makes it possible to train students in defensive cybersecurity behaviors without using harmful materials or exposing real educational systems to danger.

Chernikova et al. (2020) found that simulation-based learning in higher education can improve knowledge and skills when simulations are aligned with clear objectives, active learning tasks, feedback, and practice that is close to the target performance domain. The effectiveness of simulation does not result from the use of technology alone. It depends on the quality of task design, the degree of learner engagement, and the relationship between the activity and the intended learning outcome.

This aligns with the present study, in which Moodle was not used merely as a content delivery platform. Rather, it served as an operational environment for interactive scenarios requiring evidence inspection, decision-making, and documentation.

Vlachopoulos and Makri (2017), in their systematic review of games and simulations in higher education, similarly concluded that interactive environments may enhance student engagement and learning when learners perceive the activity as meaningful and connected to their area of study. However, this effect is not automatic. It depends on the appropriateness of the scenario, clarity of the task, balance of challenge, and alignment between interaction and learning objectives.

In the present study, such alignment was achieved by designing scenarios that belonged to the digital world of Educational Technology students: the learning platform, institutional email, cloud storage, incident reporting forms, and activity logs.

In cybersecurity training, simulations designed for non-specialist students differ from advanced cyber ranges. Cyber ranges may be used to train specialists in network analysis, defense testing, or management of complex incidents. Educational Technology students, however, require a defensive educational simulation

that focuses on safe behavior and initial decision-making. Yamin et al. (2020) noted that cybersecurity training environments vary in their objectives, functions, scenarios, and structures, and that the scenario plays a central role in determining the tasks and interactions experienced by the trainee. The present study therefore makes a clear distinction between safe educational simulation and specialized cybersecurity training environments.

Simulation is also valuable because it reveals the gap between knowledge and performance. A student may answer a knowledge question correctly but hesitate, inspect irrelevant evidence, or make an unsafe decision when facing a simulated situation. Performance rubrics and interaction logs are therefore important because they measure how students act inside the situation, not only what they know.

From a design perspective, simulation allows experience to be sequenced gradually. Students can first learn basic concepts, then interact with a simple situation, then move to a more ambiguous case, document their decision, and receive feedback. This sequencing helps reduce the gap between theoretical learning and practical action. It becomes especially important in high-realism scenarios, where students do not receive all evidence at once, but build their judgment progressively as they would in authentic digital practice.

Cyber-Threat Scenario Realism as an Instructional Design Variable

Scenario realism is one of the most sensitive components of simulation because it determines the extent to which learners feel they are engaging with a situation that resembles real practice. It also determines the extent to which the task requires cognitive and performance processes similar to those needed in actual use.

In the present study, realism does not mean adding excessive detail or making the situation unnecessarily complex. It means that the details presented in the scenario are relevant to the target skills of detection and response. A realistic scenario provides evidence that students need to inspect, includes an appropriate level of ambiguity, connects decisions to consequences, and requires justification and documentation.

Simulation literature suggests that fidelity should not be understood only as visual or technical resemblance. More importantly, fidelity should reflect alignment among task characteristics, required performance, and assessment indicators. If the objective is to develop threat detection, the relevant realism lies in the realism of the evidence, indicators, and decision pathway, not merely in the visual quality of the interface. If the objective is to develop incident response, the relevant realism lies in decision consequences, documentation, escalation, and containment rather than in the length of the story.

This perspective is supported by Chernikova et al. (2020), who emphasized that the effectiveness of simulation depends more on the design of the instructional situation, interaction, and feedback than on technical appearance alone.

In cybersecurity, the role of the scenario becomes even more central. It defines the nature of the incident, the available evidence, the decision points, the trainee's behavior, and the criteria for success. Kavak et al. (2021) argued that cybersecurity simulation requires careful modeling of the scenario, environment, user, and assessment, because weak representation of the situation may lead to learning that does not transfer effectively to real practice. This is why the present study selected scenario realism level as the independent variable: the scenario is the point at which content becomes performance.

High realism in the present study consists of several interrelated features. The first is a familiar educational context, where threats appear within a learning platform, institutional email, shared file, or activity log rather than in an abstract security setting. The second is the presence of multiple pieces of evidence, so that students do not rely on a single indicator. The third is appropriate ambiguity, because realistic digital situations are not always fully clear. The fourth is incident progression, in which indicators appear gradually. The fifth is decision consequences, because unsafe action may lead to continued data leakage, loss of evidence, or broader exposure to a suspicious link. The sixth is documentation, because a sound security decision requires justification and a written trace.

Low realism does not mean the absence of learning or poor design. Rather, it means that the situation is presented in a simpler and more direct form. The student may see a clear indicator, read a brief description, or choose an action from alternatives that involve limited ambiguity. This level may be useful during early learning, but it may be insufficient for building the ability to handle situations closer to real practice. Thus, the comparison in the present study is not between a good treatment and a weak treatment. It is a comparison between two levels of realism while controlling the content, objectives, environment, and tools.

Cognitive load theory further supports this distinction. Increasing realism should not overload learners with unnecessary information, because excessive cognitive load can weaken learning. However, when realistic details are directly related to the target skill, they become part of the essential cognitive processing required for learning rather than an irrelevant burden. Paas and van Merriënboer (2020) emphasized that instructional task design should balance complexity in a way that supports learning without exceeding learners' processing capacity. Accordingly, the present study treats high realism as controlled instructional realism, not as unstructured complexity.

Scenario realism is particularly important for Educational Technology students because the target skills are connected to situations they may actually encounter in study or future work. When students train on a situation that resembles Moodle, Google Drive, or institutional email, the likelihood of transfer to practice is stronger than when training occurs in a generic context unrelated to their field. This is consistent with literature emphasizing that task authenticity and contextual relevance are important factors in

improving learning quality and transfer to new situations (Huang et al., 2019).

Previous Studies

Studies on Security Awareness and Cybersecurity Behavior among Users

Egelman and Peer (2015) developed a scale of security behavior intentions and examined whether users' intentions could reflect their orientation toward practices such as password protection, avoiding suspicious links, and being cautious when sharing information. This study supports the present research by emphasizing that cybersecurity among non-specialists is not merely a matter of technical knowledge. It is also connected to behavior, decision-making, and readiness to act safely in everyday digital situations. It also supports the need for instruments that measure practical and behavioral dimensions rather than relying only on abstract knowledge.

McCormac et al. (2017) examined individual differences and their relationship to information security awareness. Their findings indicated that security awareness is influenced by cognitive, personal, and organizational factors, and that users do not always behave according to what they know. This finding supports the need for a simulation environment that places students inside practical situations, because knowledge alone may not ensure correct response when facing a digital threat.

Parsons et al. (2017) developed an instrument for measuring the human aspects of information security. The instrument addressed dimensions such as password management, email use, threat awareness, and information handling. This study is relevant to the present research because it confirms that secure behavior consists of small everyday practices that accumulate within digital environments. This aligns with the present study's focus on messages, links, files, permissions, and activity logs in digital learning environments.

Hadlington (2017) investigated the relationship between human factors and risky cybersecurity behaviors. The study indicated that unsafe behavior may be associated with impulsivity, digital habits, and the way users interact with technology. This supports the present study by showing that training students in response should not assume that users will always behave rationally. Instead, learners should be placed in situations that require slowing down, inspecting evidence, and making decisions before acting.

Studies on Phishing, Social Engineering, and Threat Detection

Arachchilage, Love, and Beznosov (2016) examined phishing threat avoidance behavior. The study showed that phishing avoidance is influenced by users' perception of the threat, their confidence in dealing with it, and their understanding of preventive procedures. This finding supports the present study's assumption that threat detection requires training within the situation itself. Students do not only need to know that phishing is dangerous; they need to identify the indicators that make a message or link unsafe.

Williams et al. (2018) explored users' susceptibility to phishing in workplace settings. Their findings showed that judgments about messages are influenced by context, trust, and the message's surface appearance. This study is directly relevant to the present research because many educational phishing situations may appear familiar and legitimate, particularly when they use the language of learning platforms, institutional email, or shared files.

Jampen et al. (2020), in their review of anti-phishing training, found that more effective training approaches expose users to applied examples or practice situations and provide feedback that helps them adjust behavior. This supports the use of scenario-based digital simulation in the present study, because it allows students to practice evidence inspection and decision-making within situations close to real use.

Aldawood and Skinner (2018) addressed social engineering awareness in cybersecurity and emphasized that attacks based on human deception require educational and training interventions that help users recognize psychological and social influence techniques. This study supports the inclusion of indicators such as urgency, impersonation, and requests for sensitive information in the high-realism scenarios, because these indicators are central to many social engineering situations.

Studies on Simulation and Scenario-Based Training

Vlachopoulos and Makri (2017) conducted a systematic review of games and simulations in higher education and concluded that such environments can support student learning when they are designed around clear objectives and meaningful interaction. This study supports the present research by emphasizing that digital simulation should be connected to specific learning outcomes, such as detection and response, rather than used as technology for interaction only.

Chernikova et al. (2020), in a meta-analysis of simulation-based learning in higher education, indicated that simulation is more effective when it combines practical activity, feedback, and alignment with professional or educational contexts. This supports the design of the present treatment, in which students inspected evidence, made decisions, documented responses, and received feedback within the simulation environment.

Gegenfurtner, Quesada-Pallarès, and Knogler (2020) also emphasized that practical skills require performance-based training and do not develop sufficiently through theoretical presentation or reading alone. This finding reinforces the present study's reliance on interactive scenarios and performance assessment rather than knowledge testing alone.

Studies on Cybersecurity Training Environments and Scenarios

Yamin et al. (2020) examined cybersecurity training environments, their scenarios, functions, and structures. They showed that the scenario is a central

component in cybersecurity training design because it defines situations, events, decision points, tools, and assessment indicators. This study is directly relevant to the present research because it supports viewing the scenario as an instructional design variable rather than as a simple text or story within the environment.

Kavak et al. (2021) reviewed the state of cybersecurity simulation and future directions. They concluded that cybersecurity simulation requires careful modeling of the environment, threats, user behavior, and assessment. This supports the present study by emphasizing that the quality of simulation cannot be judged merely by the existence of a digital platform. It depends on scenario quality, task clarity, and the relationship between assessment and expected behavior.

Ukwandu et al. (2020) discussed the role of cybersecurity training environments in skill development and highlighted the importance of scenarios and practical activities in enabling trainees to deal with cybersecurity situations. This is relevant to the present study because it supports the role of simulation in developing applied defensive skills, while also showing the need to adapt the design to the characteristics of the learner group.

Willems et al. (2022) emphasized that cybersecurity training experiences should consider the trainee's role, level of difficulty, degree of interaction, and type of decision required. This finding supports the distinction made in the present study between an educational simulation environment designed for Educational Technology students and advanced training environments designed for cybersecurity specialists. Different target audiences require different scenario structures and assessment tools.

Studies on Learning Analytics and Interaction Logs

Ifenthaler and Yau (2020) examined the use of learning analytics to support student success in higher education. They showed that digital interaction records can provide important indicators of learner behavior and learning pathways, not only final scores. This supports the use of the interaction analysis log in the present study, because the log measures patterns of evidence inspection, sequence of interaction, decision time, response quality, independence, and safe behavior within the simulation environment.

Viberg et al. (2018) also highlighted the importance of learning analytics in higher education for understanding student behavior and improving the design of digital learning environments. This supports the present study's decision to use interaction data as an additional source of evidence alongside tests and performance rubrics. In a simulation environment, the process by which the student reaches a decision may be as important as the final answer itself.

Synthesis of Previous Studies and Research Gap

Taken together, the previous studies show that cybersecurity learning for non-specialist users should not be limited to conceptual awareness. Studies on security behavior indicate that users' actions are shaped by attention, judgment, habits, confidence, and contextual cues. Studies on phishing and social engineering show that threats often appear in familiar and persuasive forms, which makes detection dependent on careful evidence inspection rather than simple recognition. Studies on simulation and scenario-based training indicate that practical skills develop more effectively when learners engage in meaningful tasks, receive feedback, and act within situations connected to their real contexts. Studies on cybersecurity training environments further emphasize that the scenario itself is a decisive element in defining the quality of training.

This body of literature aligns with the research problem identified in the present study, namely the weakness of Educational Technology students in detecting cyber threats and responding safely to digital incidents within educational digital situations. It also supports the use of digital simulation and scenario-based training as an appropriate instructional approach for developing these skills.

However, the literature does not sufficiently address the specific question examined in the present study. Many studies confirm the importance of simulation in general, but fewer studies isolate scenario realism as a clear independent instructional design variable. The present study therefore does not compare simulation with non-simulation. Rather, it compares two levels of scenario realism within the same digital simulation environment.

The present study differs from previous research in four main respects. First, it focuses on Educational Technology students, a group that needs defensive cybersecurity skills related to digital learning environments without being a specialist cybersecurity population. Second, it treats scenario realism level as an explicit independent variable rather than as an implicit feature of the learning environment. Third, it uses multiple instruments that measure knowledge, situated decision-making, practical performance, interaction behavior, and perceived realism. Fourth, it controls the difference between the two groups so that the only systematic variation lies in the realism level of the scenarios, not in the content, platform, time, or assessment tools.

Accordingly, the present study seeks to address a research and practical gap by examining whether high-realism scenarios within a digital simulation environment produce stronger effects than low-realism scenarios in developing cyber-threat detection and digital incident response skills among Educational Technology students.

Research Methodology and Procedures

Overview

This section presents the methodological procedures followed to examine the effect of cyber-threat scenario realism level, high-realism versus low-realism, within a digital simulation environment on developing cyber-threat detection and digital incident response skills among Educational Technology students. It describes the research method, experimental design, population and sample, variables, research instruments, development of the digital simulation environment, the

two experimental treatments, procedures for experimental control, implementation steps, and statistical methods used to analyze the data.

The procedures were designed to remain fully aligned with the title, research questions, hypotheses, and objectives of the study. Particular attention was given to avoiding any mismatch among the independent variable, dependent variables, research instruments, experimental treatment, and statistical design. The digital simulation environment was also described with methodological precision. It was not a specialized cybersecurity laboratory or cyber range. Rather, it was a safe educational simulation environment based on scenarios and designed for Educational Technology students.

Research Method

The study employed a quasi-experimental method because it was appropriate for examining the effect of a clearly defined independent variable, namely cyber-threat scenario realism level, on a set of dependent variables related to cyber-threat detection and digital incident response skills among Educational Technology students.

The quasi-experimental method was selected because the study was conducted in an existing university learning context, where full control of all variables, as in pure laboratory experiments, was not feasible. Nevertheless, the essential variables relevant to the experiment were controlled as far as possible, including instructional content, implementation platform, learning time, number of general tasks, research instruments, and pre- and post-measurement procedures. Thus, the main experimental difference between the two groups was limited to the realism level of the cyber-threat scenarios.

This methodological choice is consistent with applied research in Educational Technology, where instructional treatments are often tested within real or semi-real learning environments while maintaining the highest possible level of methodological control. It also corresponds to the nature of the present study, which does not examine simulation-based learning versus non-simulation-based learning. Instead, it examines a specific design feature within the simulation environment: the realism level of cyber-threat scenarios.

Experimental Design

The study adopted a quasi-experimental pretest–posttest design with two experimental groups. Both groups were assessed before and after the treatment using instruments measuring cyber-threat detection and digital incident response skills.

The first experimental group was exposed to high-realism cyber-threat scenarios, whereas the second experimental group was exposed to low-realism cyber-threat scenarios. The learning platform, instructional content, learning time, and research instruments were kept constant across the two groups. The perceived scenario realism scale was administered only after the treatment to both groups as a manipulation check.

Figure 2 Quasi-Experimental Design of the Study

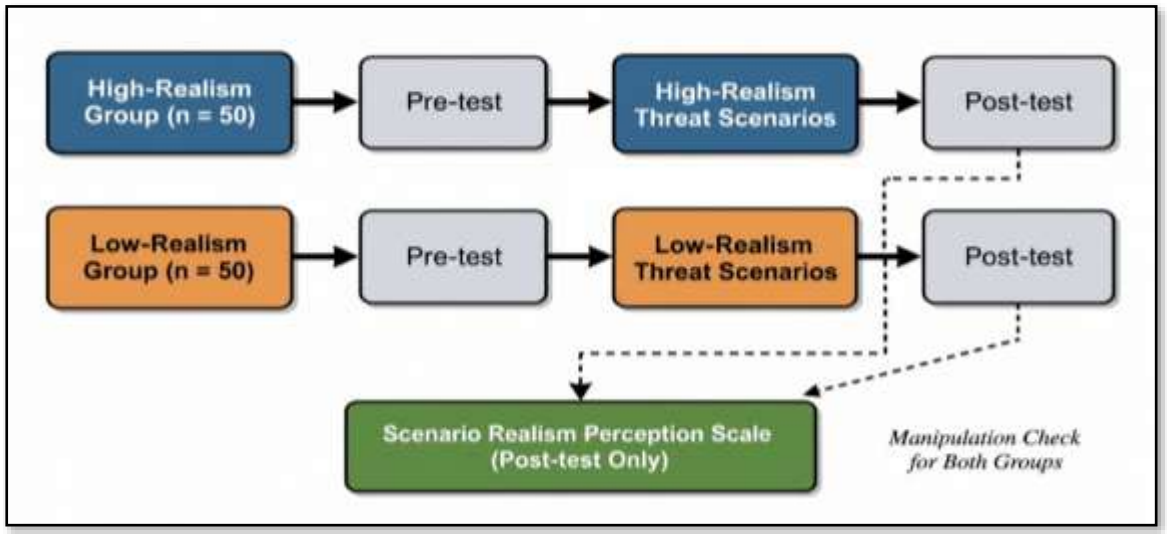


Figure 2 shows that the experimental comparison was restricted to the realism level of the threat scenarios, while the remaining elements of the experiment were controlled as far as possible. This control was necessary to attribute post-test differences between the two groups to scenario realism level rather than to differences in content, platform, learning time, or assessment tools.

Population and Sample

The study population consisted of students enrolled in the Department of Educational Technology at the Faculty of Specific Education. The main sample consisted of 100 second-level Educational Technology students during the first semester of the 2022/2023 academic year.

All participants belonged to the same academic level and specialization and had previous exposure to digital learning environments as part of their university study. None of the participants had received specialized cybersecurity training before the experimental treatment. This helped ensure that the two groups were broadly comparable in academic background and prior

exposure to the general digital learning context before the implementation of the study.

The main sample was assigned to two equivalent experimental groups, as shown in Table 1.

Table 1 Distribution of the Main Study Sample

Group	Number	Treatment Type
First experimental group	50 students	High-realism cyber-threat scenarios
Second experimental group	50 students	Low-realism cyber-threat scenarios

The study also used two supporting samples, in addition to the panel of reviewers, as shown in Table 2.

Table 2 Supporting Samples and Reviewers

Type	Number	Purpose
Exploratory sample	50 students	Diagnosing the field manifestations of the research problem and identifying the level of need for the target skills
Pilot sample	20 students	Verifying the clarity of the environment and instruments, calculating validity and reliability indicators, and reviewing implementation time
Reviewers	11 reviewers	Reviewing the skills list, scenarios, simulation environment, and measurement instruments

The pilot sample was selected from outside the main study sample so that the final implementation would not be affected by students' prior exposure to the instruments or scenarios. It was also ensured that students in the two experimental groups belonged to the same academic level and specialization and were exposed to similar general educational conditions as far as possible.

Research Variables

Independent Variable

The independent variable in the present study was:

Cyber-threat scenario realism level within the digital simulation environment.

It had two levels:

1. High-realism cyber-threat scenarios.
2. Low-realism cyber-threat scenarios.

Dependent Variables

The dependent variables were:

1. Core concepts related to cyber-threat detection and digital incident response.
2. Cyber-threat detection skills.
3. Practical performance of cyber-threat detection within the digital simulation environment.
4. Digital incident response skills.
5. Practical performance of digital incident response within the digital simulation environment.
6. Interaction quality within the digital simulation environment.

Supporting Manipulation-Check Variable

The study also used a supporting variable:

Perceived cyber-threat scenario realism.

This variable was used to verify whether students actually perceived the difference in realism between the high-realism and low-realism scenarios.

The Digital Simulation Environment

The digital simulation environment was designed as a safe scenario-based educational environment aimed at training Educational Technology students in cyber-threat detection and digital incident response within situations close to digital learning environments. The environment was operated through Moodle, with interactive activities, documentation forms, and performance records used to track students' interaction with the scenarios.

The digital simulation environment in this study was not intended to be a specialized cybersecurity laboratory or a cyber range designed for training cybersecurity experts in penetration testing, network analysis, or advanced technical incident response. Rather, it was a defensive educational simulation designed for Educational Technology students. It focused on safe skills suitable for their specialization, such as inspecting links, analyzing messages, reviewing file-sharing permissions, reading activity logs, documenting incidents, and escalating incidents to the appropriate authority.

Moodle was selected intentionally as the operational platform for the environment. It made it possible to organize students into two experimental groups, present content, run activities, administer tests, track students' attempts, and extract interaction logs. Thus, Moodle was not the simulation itself. It was the operational framework that hosted the interactive scenarios, simulated digital evidence, decision pathways, documentation forms, and performance records. Literature on digital learning environments indicates that the value of such platforms lies not only in presenting content but also in supporting interactive activities, performance tracking, feedback, and learning analytics (Ifenthaler & Yau, 2020).

All elements of the environment were designed to be safe. No real malicious links, infected files, real accounts, or actual student data were used. Students were not asked to enter personal passwords or perform any action that could put their accounts, university devices, or data at risk. In this way, the environment maintained its educational and defensive nature and avoided any offensive training or inappropriate technical practice for the study sample.

Tools and Applications Used to Build the Simulation Environment

The digital simulation environment relied on a set of safe educational tools and applications. Each had a specific function within the design, as shown in Table 3.

Table 3 Tools and Applications Used in the Digital Simulation Environment

Tool or Application	Function within the Study
Moodle	Operating and managing the digital simulation environment; organizing the two groups; providing content and activities; administering tests; extracting interaction logs
H5P within Moodle	Building interactive scenarios, decision cards, branching situations, and embedded questions within scenarios
Google Forms	Creating digital incident documentation forms, recording students' decisions, and administering the perceived scenario realism scale
Google Sheets	Organizing form responses, aggregating initial scores, and verifying the alignment between dimension scores and total scores
Google Drive	Designing simulated situations related to file-sharing settings and access permissions
Moodle logs	Tracking student activity within the environment, including access to activities, interaction time, and order of access to scenario elements
Safe or simulated checking tools	Training students in the logic of checking links and files without opening harmful elements or dealing with real threats

The use of these tools was not intended to train students to master a particular technical application. Rather, the tools were employed within a safe educational situation that helped students inspect evidence, make decisions, and document responses. This is consistent with the nature of the study, because the dependent variable was not mastery of Moodle or Google Forms, but cyber-threat detection and digital incident response skills within a simulated educational context.

The simulation environment was therefore designed as a safe educational environment that allowed students to deal with simulated cyber-threat situations related to digital learning environments without using real harmful links or files. Moodle served as the instructional host for activities, whereas the interactive scenarios, digital evidence, documentation forms, interaction logs, and assessment instruments constituted the main functional components of the environment.

Figure 3 Functional Architecture of the Digital Simulation Environment

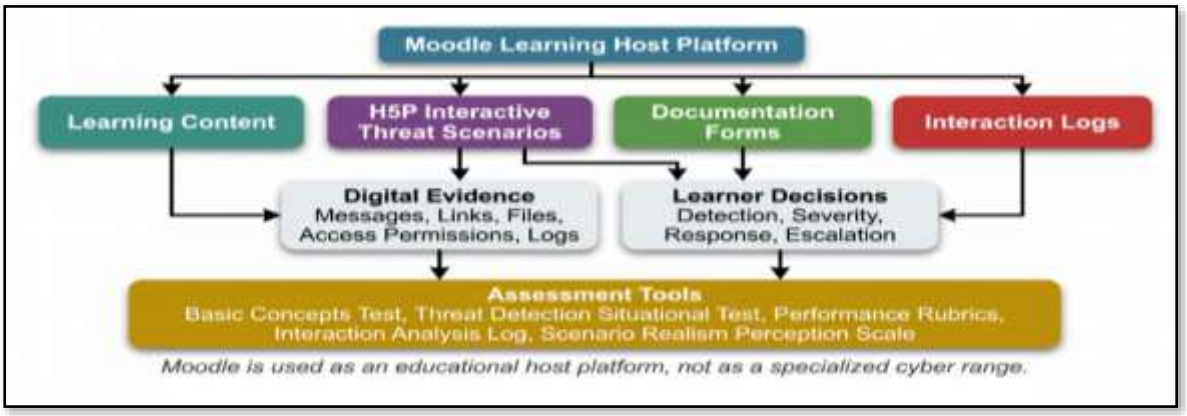


Figure 3 shows that Moodle was not used to create a specialized technical cybersecurity laboratory. Instead, it provided an organized educational framework for presenting scenarios, managing students' interaction, documenting their decisions, and analyzing their behavior within the environment. Thus, the simulation environment was directly linked to the educational aim of the study: training Educational Technology students in basic defensive skills of detection and response, not training them in offensive or advanced technical practices.

Development of the Cyber-Threat Detection and Digital Incident Response Skills List

The researcher first developed an initial list of target skills based on the nature of the research problem, the characteristics of Educational Technology students, relevant professional cybersecurity frameworks, and previous studies on security awareness, phishing, social engineering, digital simulation, and scenario-based training. The skills were selected to be suitable for Educational Technology students rather than specialized cybersecurity students.

The final list included two main domains.

Domain One: Cyber-Threat Detection Skills

This domain included the following skills:

1. Inspecting suspicious messages, links, and files within a digital educational context.

2. Collecting initial digital evidence without modifying or deleting it.
3. Analyzing suspicious indicators in messages, links, and activity logs.
4. Reviewing sharing permissions of files and digital resources.
5. Detecting phishing and impersonation attempts.
6. Detecting indicators of data leakage or unsafe access settings.
7. Identifying the type of cyber threat.
8. Estimating the severity level of the threat.
9. Distinguishing between a genuine threat and a false alarm.
10. Documenting the detection decision with evidence-based justification.

Domain Two: Digital Incident Response Skills

This domain included the following skills:

1. Conducting initial verification of the incident or suspicious situation.
2. Prioritizing the response according to severity level and scope of impact.
3. Selecting an appropriate initial response action.
4. Containing the incident and reducing its impact.
5. Preserving evidence without deleting or modifying it.
6. Documenting the incident and the actions taken.
7. Escalating the incident to the appropriate authority within the educational institution.
8. Communicating safely without sharing sensitive data or suspicious links.
9. Performing an appropriate initial recovery action.
10. Suggesting a preventive action to reduce the likelihood of recurrence.

The skills list was submitted to 11 reviewers specializing in Educational Technology, cybersecurity, and measurement and evaluation. They were asked to judge the suitability of the skills for Educational Technology students, their relevance to the study title, clarity of wording, measurability, and appropriateness for a safe digital simulation environment. Based on their comments, the wording of some skills was revised, overlapping indicators were removed, and closely related skills were merged until the list reached its final form.

Development of the Instructional Content

The instructional content was developed as a set of short, interrelated units that presented cybersecurity from an applied educational perspective suitable for Educational Technology students. The aim was not to train students in advanced technical concepts or professional cybersecurity operations. Rather, the aim was to build a knowledge base that would help them understand common threats in digital learning environments and connect that knowledge to safe behavior within situations.

The instructional content included the following units:

1. Introduction to cybersecurity in digital learning environments.
2. Common cyber threats in educational contexts.
3. Indicators of threat detection in messages, links, and files.
4. Phishing, impersonation, and social engineering.
5. Data leakage and unsafe file-sharing permissions.
6. Login records and unusual activity.
7. Initial response to digital risks and incidents.
8. Evidence preservation, documentation, and escalation.
9. Initial recovery and prevention of incident recurrence.

The instructional content was unified across the two groups so that post-test differences could not be attributed to differences in the amount or type of knowledge presented. The content was also directly linked to the scenarios. It was not presented as isolated theoretical material, but as supporting knowledge that students needed while inspecting evidence and making decisions.

Design of the Cyber-Threat Scenarios

The cyber-threat scenarios were designed in light of the skills list, instructional content, and the nature of digital learning environments with which Educational Technology students interact. The scenarios were designed to be defensive and safe, and to present situations close to everyday educational digital use rather than advanced technical situations requiring expertise in network security or penetration testing.

The scenarios included situations such as:

1. A message that appears to be sent from Moodle requesting login data update.
2. A fake link to attend a virtual meeting.
3. A Google Drive file containing educational data and shared with public permissions.
4. An unusual login record for a student account within the learning platform.
5. An impersonation message requesting files or student data.
6. An attachment with an educational name but containing risk indicators.
7. A simulated alert about a login attempt from an unfamiliar device.
8. A situation requiring incident documentation and escalation to the appropriate authority.

Each scenario included one or more detection skills and one or more response skills. Students were therefore required to move from noticing an indicator to making a safe decision.

Student interaction within the scenario was not based on selecting a direct answer only. It involved a sequence of performance-based steps beginning with reading the digital situation, inspecting evidence, making a detection decision, choosing a response action, documenting the evidence and reasoning behind the decision, and receiving safe educational feedback.

Figure 4 Learner Interaction Pathway within a Threat Scenario

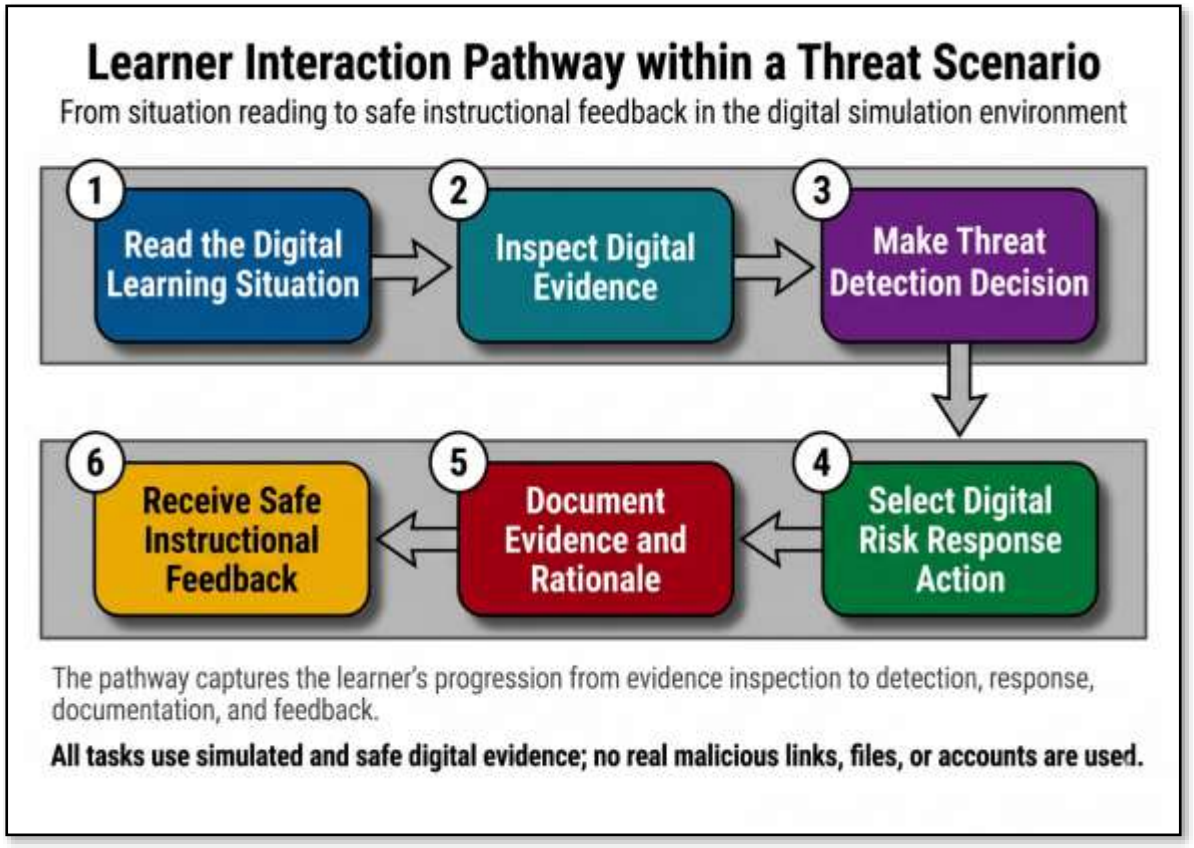


Figure 4 shows that the scenario was not used merely as an instructional story. It functioned as an organized performance structure that required students to inspect, analyze, decide, respond, and document. This pathway is consistent with the nature of educational cybersecurity skills because such skills are not measured simply by knowing a term, but by the student's ability to read a digital situation and act within it in a safe and justified manner.

First Experimental Treatment: High-Realism Scenarios

The first experimental treatment was designed to present high-realism cyber-threat scenarios within the digital simulation environment. The aim of this treatment was to place students in digital educational situations that were close to real practice, where the risk was not obvious from the beginning and the correct response could not be selected without inspection.

The high-realism scenarios were characterized by the following features:

1. **Realistic educational context:** Threats appeared within a learning platform, institutional email, shared file, activity log, or virtual meeting.
2. **Multiple digital evidence sources:** The scenario did not depend on a single indicator. It included elements such as sender address, link, message text, timing, activity log, sharing permissions, or attachment.
3. **Appropriate ambiguity:** Not every situation appeared as a confirmed threat from the outset; students had to analyze the evidence before making a judgment.
4. **Incident progression:** Indicators appeared gradually, moving the student from suspicion to verification and then to decision-making.
5. **Decision consequences:** Students' choices led to an educational consequence within the scenario, such as continued risk, loss of evidence, reduced impact, or correct documentation.
6. **Mandatory documentation:** The task did not end with selecting an answer. Students were required to record the threat type, evidence, severity level, action taken, and appropriate escalation authority.
7. **Educational feedback:** Students received feedback explaining the quality of their decision and its security implications.

An example of a high-realism scenario involved a student receiving a message that appeared to be from a Moodle administrator asking them to review unusual account activity. The message used a familiar logo, but the sender's email address contained a slight difference from the official domain. When previewing the link, the student found that it led to a page resembling the original login page, but not hosted on the university domain. The scenario also displayed an activity log showing a login attempt from an unfamiliar device. In this situation, the student could not rely on one indicator only. They needed to inspect the sender address, link, activity log, and nature of the request before deciding the type of threat, its severity, and the appropriate response action.

Second Experimental Treatment: Low-Realism Scenarios

The second experimental treatment was designed to present low-realism cyber-threat scenarios within the same digital simulation environment. This treatment presented the same content and target skills, but the situations were simpler and more direct. The evidence was fewer, ambiguity was limited, and the decision pathway was shorter.

The low-realism scenarios were characterized by the following features:

1. **Simplified educational context:** The situation was presented as a direct description or a short activity.
2. **Limited evidence:** Risk indicators appeared clearly and directly.
3. **Low ambiguity:** The threat was usually easier to classify than in the high-realism scenario.
4. **Linear pathway:** The situation did not require movement among multiple evidence sources or sequential verification steps.
5. **Less detailed consequences:** Decision outcomes were not presented with the same depth as in the high-realism scenarios.
6. **Brief documentation:** Students recorded the decision, but they were not required to make an extended connection among multiple pieces of evidence.

An example of a low-realism scenario was a direct description of a message asking the student to enter a password through an unknown link, followed by a request to identify the threat type and select the appropriate response. In this scenario, the risk indicators were more explicit, and the student did not need to inspect multiple pieces of evidence or follow a complex incident sequence.

Low realism did not mean that the treatment was weak or non-educational. It meant that the situation was less close to reality in terms of evidence structure, ambiguity, incident sequence, and decision consequences. The purpose of this design was to test whether high realism adds genuine educational value beyond training through simplified situations.

Scenario realism in the present study was represented through several design dimensions, including the realism of the digital learning context, nature of evidence, degree of ambiguity, incident sequence, decision consequences, documentation requirements, and scenario pathway. Both groups used the same platform, content, objectives, learning time, and measurement instruments. The difference between them was restricted to the realism level of the scenarios.

Figure 5 Design Contrast between High- and Low-Realism Threat Scenarios

The two treatments were identical in platform, content, objectives, time, and measurement tools; only scenario realism differed.

High-Realism Threat Scenarios	Design Dimension	Low-Realism Threat Scenarios
Authentic educational contexts such as LMS, university email, cloud storage, virtual meetings, and activity logs	Digital Learning Context	Simplified educational context presented in a more direct form
Multiple and distributed indicators requiring careful evidence inspection	Digital Evidence	Limited and explicit indicators that are easier to identify
Moderate and realistic ambiguity that requires interpretation before judgment	Ambiguity Level	Low ambiguity with relatively obvious threat cues
Gradual development of the incident across sequential cues	Incident Sequence	Short and direct situation with fewer sequential cues
Clear consequences linked to learner decisions and response actions	Decision Consequences	Less detailed consequences associated with learner decisions
Detailed evidence-based documentation of threat type, severity, rationale, and response	Documentation Requirement	Brief documentation focused mainly on the final answer or selected action
Branching or semi-branching pathway with decision points	Scenario Path	Mostly linear pathway with limited decision branching

Controlled Elements: Moodle platform, learning content, instructional objectives, learning time, number of tasks, and assessment tools.

Figure 5 shows that high-realism scenarios provided more authentic digital educational contexts, multiple and distributed evidence sources, ambiguity requiring interpretation, gradual incident progression, clear decision consequences, and detailed evidence-based documentation. By contrast, low-realism scenarios presented more direct and less ambiguous situations, with limited evidence and a more linear pathway. The difference between the two treatments should therefore not be understood as a difference in content quantity, but as a difference in the design realism of the learning experience.

Control of Differences between the Two Experimental Treatments

The study carefully controlled differences between the two experimental groups so that the results would not be attributable to differences in content, platform, time, or measurement instruments. Both groups studied the same content, used Moodle, were exposed to the same

skills, completed the same pre- and post-measures, and had equivalent learning time.

The elements of experimental control are shown in Table 4.

Table 4 Control of Design Elements across the Two Experimental Treatments

Design Element	High-Realism Group	Low-Realism Group
Platform	Moodle	Moodle
Scenario-building tool	H5P within Moodle	H5P within Moodle
Instructional content	Unified	Unified
Learning objectives	Unified	Unified
Learning time	Unified	Unified
Number of general tasks	Equivalent	Equivalent
Measurement instruments	Unified	Unified
Threat types	Unified in topic	Unified in topic
Realism level	High	Low
Evidence	Multiple and distributed	Limited and direct
Ambiguity	Appropriate and close to reality	Limited
Incident sequence	Gradual	Brief
Decision consequences	Clear and contextually connected	Less detailed
Scenario pathway	Relatively branching	More direct

Thus, the experimental difference was controlled around scenario realism level, not the amount of learning, platform quality, or assessment tools.

Research Instruments

The study used seven instruments designed to measure the dependent variables from cognitive, situational, performance-based, and behavioral perspectives, in addition to an instrument for verifying students' perception of the realism of the experimental treatment. The use of multiple instruments was necessary because cyber-threat detection and digital incident response are complex skills that cannot be measured accurately through a single knowledge test.

The study adopted a multi-source assessment system so that judgment of the treatment effect would not be based on a single cognitive instrument. The instruments measured cognitive, situational, performance-based, and behavioral dimensions, in addition to students' perception of scenario realism.

Figure 6 Measurement Map of the Study

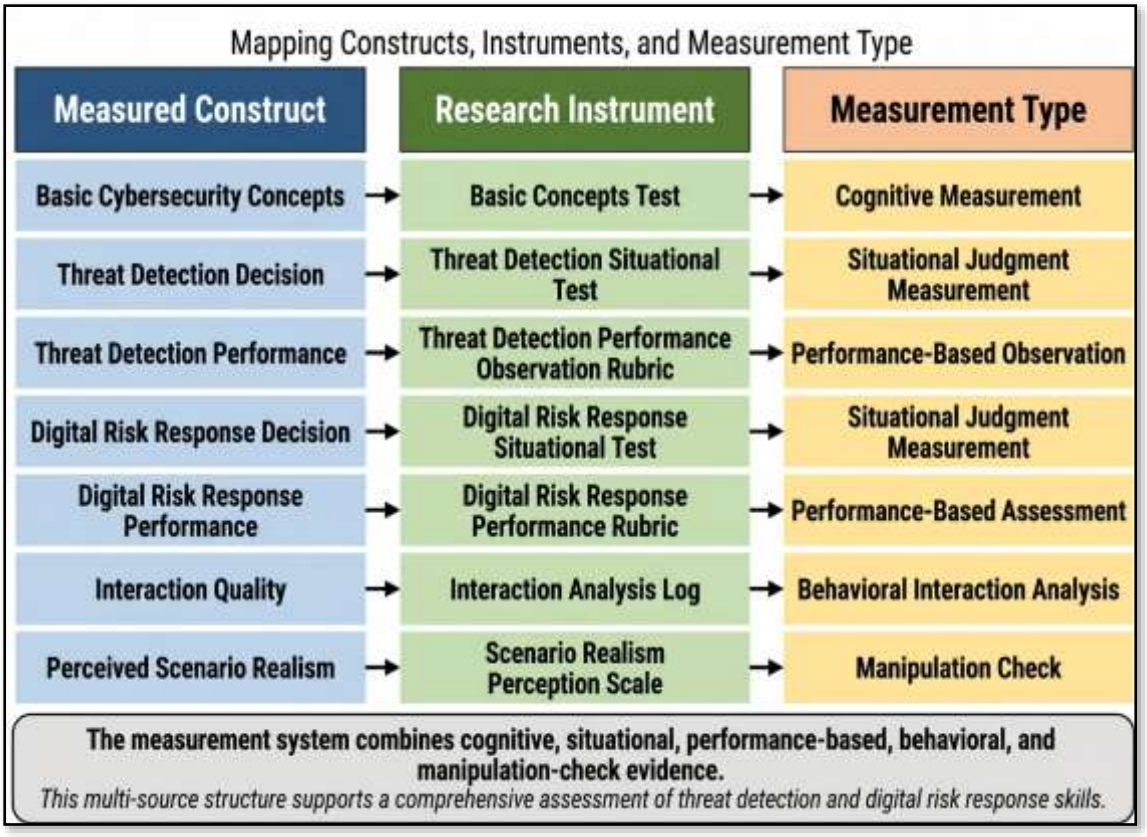


Figure 6 shows that the research instruments covered multiple levels of learning and performance. The core concepts test measured the cognitive dimension. The situational tests measured detection and response

decisions. The performance rubrics measured practical behavior within the environment. The interaction analysis log provided behavioral evidence of interaction quality. The perceived realism scale was used to verify that students recognized the difference in realism level between the two treatments.

Instrument 1: Test of Core Concepts Related to Cyber-Threat Detection and Digital Incident Response

This test measured the cognitive dimension related to the basic concepts required for cyber-threat detection and digital incident response. It consisted of 40 items distributed across six dimensions: cybersecurity and digital incident concepts, common cyber-threat types, indicators of threat detection, incident classification and severity estimation, initial response procedures, and documentation, escalation, and evidence preservation.

The instrument was designed to measure knowledge supporting performance, not as a substitute for measuring practical performance.

Instrument 2: Cyber-Threat Detection Situational Test

This test measured students' ability to apply knowledge within suspicious digital educational situations. It consisted of 20 situations distributed across five dimensions: detecting threats in messages and links, credential theft and social engineering, indicators of malware and account compromise, data leakage and misuse of access permissions, and severity estimation with distinction between genuine and false alerts.

The maximum score was 40. The reliability analysis showed a KR-20 coefficient of 0.88 and a split-half reliability coefficient of 0.85.

Instrument 3: Performance Observation Rubric for Cyber-Threat Detection within the Digital Simulation Environment

This rubric measured students' practical performance while detecting threats within the simulation environment. It consisted of five dimensions and 30 performance indicators, with a total raw score of 120. The raw score was used in statistical analyses, although it could be converted into a percentage for descriptive presentation.

The dimensions were: inspecting scenario elements and collecting evidence, analyzing suspicious indicators, identifying the type of threat, estimating threat severity, and documenting the detection decision. Cronbach's alpha was 0.91, and the Kappa coefficient for inter-rater agreement was 0.84, indicating a high and appropriate level of reliability.

Instrument 4: Digital Incident Response Situational Test

This test measured students' ability to select appropriate response decisions when facing digital incidents or risks in educational environments. It consisted of 20 situations distributed across five dimensions: initial verification and prioritization, incident containment and impact reduction, evidence preservation and initial documentation, escalation and secure communication, and initial recovery and prevention of recurrence.

The maximum score was 40. The KR-20 coefficient was 0.87, and the split-half reliability coefficient was 0.84.

Instrument 5: Digital Incident Response Performance Assessment Rubric within the Digital Simulation Environment

This rubric measured students' practical performance when responding to digital risks and incidents within the simulation environment. It consisted of five dimensions and 30 performance indicators, with a total raw score of 120. The raw score was used in statistical analyses, although it could be converted into a percentage for descriptive purposes.

The dimensions were: initial verification and prioritization, incident containment and impact reduction, evidence preservation and practical documentation, escalation and secure communication, and initial recovery and prevention of recurrence. Cronbach's alpha was 0.90, and the Kappa coefficient for inter-rater agreement was 0.86.

Instrument 6: Interaction Analysis Log within the Digital Simulation Environment

The interaction analysis log measured students' actual behavior while interacting with the simulation scenarios. It consisted of five dimensions and 20 indicators, with a raw score of 80 that could be converted to 100. The dimensions were: pattern of digital evidence inspection, threat detection accuracy, incident response quality, performance and time efficiency, and independence, safe behavior, and documentation.

Cronbach's alpha was 0.89, and the Kappa coefficient for analyst agreement was 0.85.

Instrument 7: Perceived Cyber-Threat Scenario Realism Scale

This scale verified students' perception of the realism level of the scenarios they experienced. It served as a manipulation-check instrument rather than as a primary dependent variable in the same sense as the other instruments.

The scale consisted of 30 statements distributed across six dimensions: realism of threat context, realism of evidence and indicators, realism of incident sequence, realism of inspection and response tools, realism of time pressure and decision consequences, and realism of ambiguity and decision-making. Cronbach's alpha was 0.89, and the split-half reliability coefficient was 0.86.

Validity of the Research Instruments

The validity of the research instruments was verified through content validity. The instruments were submitted to 11 reviewers specializing in Educational Technology, cybersecurity, and measurement and evaluation. The reviewers were asked to judge the extent to which the items and indicators were related to their intended dimensions, their suitability for

Educational Technology students, clarity of wording, quality of response alternatives, and appropriateness for use within a safe educational digital simulation environment.

Content validity indicators showed high values. The S-CVI/Ave reached 0.93 for the threat detection observation rubric, 0.93 for the response performance assessment rubric, 0.93 for the interaction analysis log, and 0.93 for the perceived scenario realism scale. These values indicate a high level of agreement among reviewers regarding the suitability of the instruments for measuring their intended constructs.

Based on reviewers' comments, some wording was revised for greater clarity, some technical terms were simplified to suit Educational Technology students, performance indicators were adjusted to measure practical behavior rather than knowledge alone, and some scenarios were modified to ensure security safety and direct relevance to digital educational contexts.

Reliability of the Research Instruments

The reliability of the instruments was verified by administering them to a pilot sample of 20 students who were not included in the main sample. Reliability coefficients appropriate to each instrument were used. KR-20 and split-half reliability were used for the objective and situational tests. Cronbach's alpha was used for multi-indicator rubrics and scales. Inter-rater agreement coefficients were used for the performance rubrics and interaction log.

Table 5 Reliability Coefficients of the Research Instruments

Instrument	Reliability Coefficient
Cyber-threat detection situational test	KR-20 = 0.88; split-half = 0.85
Digital incident response situational test	KR-20 = 0.87; split-half = 0.84
Performance observation rubric for threat detection	Cronbach's alpha = 0.91; Kappa = 0.84
Digital incident response performance assessment rubric	Cronbach's alpha = 0.90; Kappa = 0.86
Interaction analysis log	Cronbach's alpha = 0.89; Kappa = 0.85
Perceived scenario realism scale	Cronbach's alpha = 0.89; split-half = 0.86

The reliability of the observation and assessment rubrics was also calculated between two independent raters. The intraclass correlation coefficient reached 0.87 for the threat detection rubric and 0.86 for the response rubric. Cooper's agreement percentage was 86.4% for the detection rubric and 85.7% for the response rubric. These values indicate a high and acceptable level of rater agreement.

Pilot Experiment

A pilot experiment was conducted with 20 students from outside the main sample. The purpose of the pilot was to verify the clarity of the simulation environment instructions, ease of access to Moodle, students' ability to deal with H5P activities, clarity of documentation forms, suitability of scenario implementation time, smooth movement between activity pages, clarity of measurement instruments, and validity of the interaction logs.

The pilot results showed that students were able to use the environment and activities, that task completion time was appropriate, and that the instrument instructions were clear. Validity and reliability results also indicated that the instruments were suitable for final implementation after making minor linguistic and organizational adjustments.

Orientation before the Main Implementation

Before the main implementation, the researcher held an orientation session for students. The session introduced the idea of the digital simulation environment, explained how to access Moodle, how to interact with the activities, how to complete documentation forms, and how to take the tests. The researcher also emphasized that all scenarios were safe and simulated and did not include harmful links, infected files, or real accounts.

The orientation session did not disclose the nature of the difference between high-realism and low-realism scenarios so that students' responses or perceptions of the treatment would not be influenced in advance. Students were also informed that the purpose of the activities was to inspect evidence and make decisions, not to guess quickly or search for a superficial answer.

Ethical and Security Considerations

Several ethical and security procedures were followed throughout the study. Participation was voluntary, and students were informed that the activities were designed for educational and research purposes. The researcher clarified that the scenarios used in the digital simulation environment were simulated, safe, and did not include malicious links, infected files, real compromised accounts, or harmful code.

Students were not asked to enter personal passwords, disclose sensitive information, or interact with any real cyber threat. All messages, links, files, accounts, activity logs, and digital evidence used in the scenarios were fictional or simulated. The environment was therefore limited to defensive educational practices, such as evidence inspection, safe decision-making, incident documentation, and escalation to the appropriate authority.

To protect participants' privacy, students' data were coded using numbers instead of names. The data were analyzed in aggregate form and used only for research purposes. The study did not involve offensive cybersecurity training, penetration testing, exploitation techniques, malware analysis, or any procedure that could expose students, university systems, or institutional data to risk.

These procedures were necessary because the study addressed cybersecurity-related learning within an educational context. The aim was to provide realistic but safe learning experiences, ensuring that scenario

realism did not compromise ethical or digital safety requirements.

Pre-Measurement

The research instruments were administered to both groups before exposure to the experimental treatment. The pre-measurement included the following instruments:

1. Test of core concepts related to cyber-threat detection and digital incident response.
2. Cyber-threat detection situational test.
3. Performance observation rubric for threat detection within a pre-simulation task.
4. Digital incident response situational test.
5. Response performance assessment rubric within a pre-simulation task.
6. Interaction analysis log within the simulation environment.

The pre-measurement results were used to verify the equivalence of the two groups and were later used in analysis of covariance when adjustment for pretest scores was needed.

Implementation of the Experimental Treatment

The experimental treatment was implemented over eight academic weeks during the first semester of the 2022/2023 academic year. Learning and implementation time were unified across both groups. Students in both groups were exposed to the same number of weeks, the same number of sessions, and tasks equivalent in their general objectives.

Each session followed a semi-fixed structure:

1. A brief introduction to the target concept or skill.
2. Presentation of a simulation situation within Moodle.
3. Student interaction with an H5P activity.
4. Inspection of digital evidence available within the scenario.
5. Making a threat detection decision.
6. Selecting the appropriate response action.
7. Documenting the decision through an electronic form.
8. Receiving safe educational feedback.
9. Saving activity data and interaction records.

The difference between the two groups was that the high-realism group interacted with scenarios richer in evidence, more ambiguous, and more strongly connected to decision consequences. The low-realism group interacted with simpler and less branching scenarios, while content, objectives, time, and instruments remained constant.

Student Interaction Mechanism within Each Scenario

Students passed through five main steps within each scenario.

1. Reading the Situation

The student read a description of a digital educational situation, such as an email message, link, shared file, activity log, or alert inside a learning platform.

2. Inspecting Evidence

The student inspected available evidence, such as sender address, link, file type, sharing permissions, login record, or message text.

3. Detection Decision

The student determined whether the situation represented a confirmed threat, a potential threat, a false alarm, or a case requiring further verification.

4. Response Decision

The student selected the appropriate action, such as not opening the link, preserving evidence, restricting permissions, changing the password through an official channel, escalating to the appropriate authority, or documenting the incident.

5. Documentation

The student recorded the decision, evidence used, threat type, severity level, action taken, and appropriate escalation authority.

These steps made the student deal with the scenario as a practical situation requiring inspection, decision-making, and justification, rather than as a theoretical question.

Ethical and Security Considerations

The study followed a set of ethical and security considerations during implementation. Students were informed that all scenarios used in the environment were simulated and safe and that they did not include harmful links, infected files, or real accounts. Students were not asked to enter personal passwords or sensitive data. Fictional names, records, and files were used within the scenarios.

All digital evidence used in the simulation environment was simulated and safe. No harmful links, infected files, or real accounts at risk were included. Students' data were treated confidentially, and their results were used only for research purposes. Clear instructions emphasized that the purpose of implementation was learning and training, not punitive evaluation.

Students' data were coded using numbers instead of names. The environment activities were limited to defensive educational skills, such as evidence inspection, incident documentation, and appropriate escalation. No offensive practices or actions that could expose students or university systems to risk were included.

These considerations are essential in educational cybersecurity research because training on digital incidents must balance realism with safety. A scenario should feel close to reality, but it should not expose learners or the institution to actual risk.

Data Extraction and Organization

Research data were extracted from three main sources:

1. **Moodle:** to extract activity scores, student attempts, login and interaction logs, and access time for activities.
2. **Electronic documentation forms:** to extract students' decisions, the evidence they recorded, the response procedures they selected, and responses to the perceived realism scale.

3. **Spreadsheet files:** to organize responses, review scores, and verify that dimension scores matched total scores.

Before conducting the final statistical analysis, the researcher reviewed the data files to ensure completeness, absence of missing values in the main scores, absence of scores exceeding the maximum limits of any instrument or dimension, correspondence between dimension totals and total instrument scores, correct coding of the two groups, and accurate entry of pre- and post-measurement scores.

A final verification step was conducted to ensure that all scores corresponded to the maximum score of each instrument and that no dimension score exceeded its expected range. Group coding was also checked before analysis to avoid reversing the high-realism and low-realism groups. For instruments scored by raters, score sheets were compared with the final data file to ensure that the entered scores matched the original rating forms.

Statistical Procedures

Before applying the statistical tests, the suitability of the data for analysis was reviewed in terms of measurement type, independence of observations, approximate homogeneity of variances, and suitability of using independent-samples t-tests and analysis of covariance. The results were interpreted in light of means, standard deviations, and effect sizes, not statistical significance alone.

The following statistical methods were used:

1. Means and standard deviations to describe students' performance on the research instruments.
2. Independent-samples t-tests to examine differences between the two groups in pre- and post-measurements.
3. Paired-samples t-tests, when needed, to compare pre- and post-measurements within the same group.
4. Analysis of covariance (ANCOVA) to control for the effect of pre-measurement when interpreting post-test differences.
5. Cohen's d to estimate the practical strength of differences between the two groups.
6. Partial eta squared to estimate treatment effect size in ANCOVA.
7. KR-20 and split-half reliability to calculate the reliability of tests.
8. Cronbach's alpha to calculate the reliability of multi-indicator instruments.
9. Intraclass correlation coefficient, Cohen's Kappa, and Cooper's agreement percentage to verify inter-rater agreement in the performance rubrics.

The interpretation of results did not rely on statistical significance alone. It also considered effect size, consistency of findings across instruments, and the nature of the measured variables. This is important for studies submitted to high-ranking scientific journals, because statistical significance may be influenced by sample size, whereas effect size helps clarify the practical strength of the treatment.

Cohen's d was used as the main standardized effect size index for between-group differences. Because the two experimental groups were equal in size and each included 50 participants, Cohen's d was considered an appropriate estimate for the practical magnitude of the differences. Future reporting may also include Hedges' g and confidence intervals for effect sizes to provide more conservative estimates of practical significance.

Summary of Research Procedures

The study followed a systematic sequence that began with field diagnosis of the research problem, followed by the development of the skills list, instructional content, digital simulation environment, high- and low-realism scenarios, and research instruments. The instruments were then reviewed, piloted, and administered before and after the treatment to the main sample.

The researcher maintained consistency between the two groups in platform, content, time, objectives, and measurement instruments. The experimental difference was limited to the realism level of the cyber-threat scenarios. Accordingly, the research procedures were consistent with the study title, hypotheses, variables, and main objective: examining the effect of cyber-threat scenario realism level on developing cyber-threat detection and digital incident response skills among Educational Technology students.

Results

Assumption Checks

Before conducting the main statistical analyses, the dataset was screened to verify the suitability of the selected statistical procedures. The data were reviewed for missing values, out-of-range scores, coding errors, and extreme values. No invalid total scores were found, and all instrument scores fell within their expected scoring ranges.

The assumptions of independent observations and approximate normality were considered acceptable because the participants were assigned to two independent experimental groups, and the sample size in each group was sufficient for the planned parametric analyses. Homogeneity of variance was examined before conducting independent-samples t-tests. When interpreting the results of ANCOVA, the relationship between pretest and posttest scores was reviewed to ensure that the covariate was relevant to the posttest outcome.

ANCOVA was used to control for pretest differences when needed, particularly for the interaction analysis log, where a statistically significant pretest difference appeared between the two groups. This procedure helped reduce the influence of initial differences and supported a more accurate interpretation of the posttest treatment effect.

Preliminary Analysis: Equivalence of the Two Groups before the Treatment

Before testing the research hypotheses, the equivalence of the two experimental groups was examined in the pre-measurement of the main dependent variables.

Independent-samples t-tests were used to compare the pretest scores of the high-realism scenario group and the low-realism scenario group.

Table 6 Pretest Equivalence of the Two Experimental Groups

Instrument	Group	N	Mean	SD	t	p	Significance
Core concepts test	High-realism	50	20.68	3.48	0.260	0.795	Not significant
	Low-realism	50	20.52	2.60			
Cyber-threat detection situational test	High-realism	50	18.76	3.72	-1.838	0.069	Not significant
	Low-realism	50	20.18	4.00			
Performance observation rubric for cyber-threat detection	High-realism	50	46.88	6.12	-0.864	0.390	Not significant
	Low-realism	50	47.92	5.92			
Digital incident response situational test	High-realism	50	19.18	3.46	-1.139	0.258	Not significant
	Low-realism	50	19.96	3.39			
Digital incident response performance assessment rubric	High-realism	50	47.58	5.70	-0.813	0.418	Not significant
	Low-realism	50	48.48	5.37			
Interaction analysis log	High-realism	50	38.30	4.78	-2.053	0.043	Significant in favor of the low-realism group
	Low-realism	50	39.86	2.45			

Table 6 shows that the pretest differences between the two groups were not statistically significant for most research instruments, namely the core concepts test, the cyber-threat detection situational test, the performance observation rubric for cyber-threat detection, the digital incident response situational test, and the digital incident response performance assessment rubric. This indicates that the two groups were largely equivalent before the implementation of the experimental treatment.

However, a statistically significant pretest difference was found in the interaction analysis log, in favor of the low-realism scenario group. For this reason, ANCOVA was used when interpreting the post-treatment results of the interaction analysis log in order to control for the effect of the pretest difference and to ensure that posttest differences were attributable to the experimental treatment rather than to initial group differences.

Hypothesis Testing

First Hypothesis

The first hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the test of core concepts related to cyber-threat detection and digital incident response, in favor of the high-realism scenario group.

To test this hypothesis, means and standard deviations were calculated, and an independent-samples t-test was conducted.

Table 7 Independent-Samples t-Test for Posttest Differences in the Core Concepts Test

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	33.98	2.86	15.834	< .001	3.17
Low-realism	50	25.38	2.56			

Table 7 shows a statistically significant posttest difference between the two groups in the core concepts test, in favor of the high-realism scenario group. The mean score of the high-realism group was 33.98, compared with 25.38 for the low-realism group. Cohen's d was 3.17, indicating a very large effect size. This suggests that the difference was not only statistically significant but also practically substantial.

To further verify the effect of the treatment after controlling for pretest scores, ANCOVA was conducted.

Table 8 ANCOVA Results for the Effect of Treatment on the Core Concepts Test

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	278.981	< .001	0.742

Table 8 shows that the treatment effect remained statistically significant after controlling for pretest scores, $F = 278.981$, $p < .001$, with a partial eta squared value of 0.742. This indicates a large treatment effect. Accordingly, the first hypothesis was accepted.

To provide a more detailed interpretation of the results, posttest differences were also examined across the dimensions of the core concepts test.

Table 9 Posttest Differences between the Two Groups across the Dimensions of the Core Concepts Test

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Cybersecurity and digital incident concepts	4.44	1.70	3.88	0.66	2.17	0.033	0.43
Common cyber-threat types	5.78	1.85	4.92	0.70	3.07	0.003	0.61
Threat detection indicators	7.40	1.05	6.06	0.65	7.67	< .001	1.53
Incident classification and severity estimation	5.62	0.57	4.50	0.51	10.42	< .001	2.08
Initial response procedures	7.52	0.86	4.26	0.92	18.26	< .001	3.65
Documentation, escalation, and evidence preservation	3.22	1.53	1.76	0.77	6.03	< .001	1.21

Table 9 indicates that the high-realism group outperformed the low-realism group across all dimensions of the core concepts test. The largest differences appeared in initial response procedures, incident classification and severity estimation, threat detection indicators, and documentation, escalation, and evidence preservation. This pattern suggests that high-realism scenarios did not merely improve students' general knowledge; they particularly strengthened knowledge elements that are closely connected to practical decision-making and safe response.

Second Hypothesis

The second hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the cyber-threat detection situational test, in favor of the high-realism scenario group.

Table 10 Independent-Samples t-Test for Posttest Differences in the Cyber-Threat Detection Situational Test

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	32.50	2.82	10.843	< .001	2.17
Low-realism	50	25.78	3.35			

Table 10 shows a statistically significant posttest difference between the two groups in the cyber-threat detection situational test, in favor of the high-realism scenario group. The effect size was very large, Cohen's $d = 2.17$, indicating that the high-realism scenarios had a strong effect on students' ability to deal with threat detection situations.

ANCOVA was then used to verify the treatment effect after controlling for pretest scores.

Table 11 ANCOVA Results for the Effect of Treatment on the Cyber-Threat Detection Situational Test

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	112.619	< .001	0.537

Table 11 shows that the treatment effect remained statistically significant after adjusting for pretest scores, $F = 112.619$, $p < .001$, with a partial Eta squared value of 0.537. This indicates a large effect. Accordingly, the second hypothesis was accepted.

The dimensions of the cyber-threat detection situational test were also examined.

Postte

Table 12 st Differences between the Two Groups across the Dimensions of the Cyber-Threat Detection Situational Test

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Detecting threats in messages and links	6.26	1.48	5.06	1.75	3.69	< .001	0.74
Credential theft and social engineering	6.52	1.50	5.30	1.80	3.68	< .001	0.74
Indicators of malware and account compromise	6.70	1.40	5.30	1.66	4.56	< .001	0.91
Data leakage and misuse of access permissions	6.28	1.36	5.22	1.95	3.15	0.002	0.63
Severity estimation and distinction between genuine and false alerts	6.74	1.37	4.90	1.69	5.98	< .001	1.20

The results in Table 12 show that the high-realism group achieved higher scores across all dimensions of the cyber-threat detection situational test. The largest effect was found in severity estimation and distinguishing between genuine and false alerts. This is methodologically important because this dimension requires deeper judgment than simple recognition. It suggests that high-realism scenarios helped students interpret evidence and evaluate the seriousness of a situation more effectively.

Third Hypothesis

The third hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the performance observation rubric for cyber-threat detection within the digital simulation environment, in favor of the high-realism scenario group.

Table 13 Independent-Samples t-Test for Posttest Differences in the Cyber-Threat Detection Performance Rubric

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	102.92	6.10	36.022	< .001	7.20
Low-realism	50	68.46	2.92			

Table 13 shows a statistically significant difference between the two groups in practical cyber-threat detection performance, in favor of the high-realism scenario group. The mean score of the high-realism group was 102.92, compared with 68.46 for the low-realism group. Cohen's d was 7.20, indicating an extremely large effect size.

Although the effect size was very large, it should be interpreted in light of the performance-based nature of the instrument. The rubric measured behaviors that were directly practiced within the high-realism scenarios, including evidence inspection, indicator analysis, threat classification, severity estimation, and documentation. The magnitude of the difference therefore reflects the close alignment between the instructional treatment and the assessed performance, rather than a general claim that scenario realism alone would produce the same effect across all contexts.

ANCOVA was used to verify the treatment effect after controlling for pretest scores.

Table 14 ANCOVA Results for the Effect of Treatment on Cyber-Threat Detection Performance

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	1278.505	< .001	0.929

Table 14 indicates that the effect of the treatment remained statistically significant after controlling for pretest scores, $F = 1278.505$, $p < .001$. The partial Eta squared value was 0.929, indicating a very strong treatment effect. Accordingly, the third hypothesis was accepted.

The dimensions of the cyber-threat detection performance rubric were also analyzed.

Table 15 Posttest Differences between the Two Groups across the Dimensions of the Cyber-Threat Detection Performance Rubric

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Inspecting scenario elements and collecting evidence	21.40	1.59	14.54	0.73	27.69	< .001	5.54
Analyzing suspicious indicators	25.60	1.59	17.32	0.84	32.51	< .001	6.50

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Identifying threat type	22.58	1.16	14.70	0.86	38.49	< .001	7.70
Estimating threat severity	21.04	1.43	13.80	0.67	32.46	< .001	6.49
Documenting the detection decision	12.30	0.71	8.10	0.30	38.60	< .001	7.72

Table 15 shows that the high-realism group outperformed the low-realism group in all performance dimensions. The strongest differences appeared in documenting the detection decision and identifying the threat type. This indicates that high-realism scenarios helped students move from general awareness to evidence-based justification, which is essential in practical cybersecurity-related decision-making.

Fourth Hypothesis

The fourth hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the digital incident response situational test, in favor of the high-realism scenario group.

Table 16 Independent-Samples t-Test for Posttest Differences in the Digital Incident Response Situational Test

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	33.46	3.02	12.225	< .001	2.44
Low-realism	50	26.14	2.97			

Table 16 shows a statistically significant posttest difference between the two groups in the digital incident response situational test, in favor of the high-realism scenario group. Cohen's d was 2.44, indicating a very large effect. This means that the high-realism treatment was more effective in helping students choose appropriate responses to digital incidents.

ANCOVA was conducted to control for pretest scores.

Table 17 ANCOVA Results for the Effect of Treatment on the Digital Incident Response Situational Test

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	149.973	< .001	0.607

Table 17 indicates that the treatment effect remained statistically significant after controlling for pretest scores, $F = 149.973$, $p < .001$, with a partial Eta squared value of 0.607. This indicates a large effect. Accordingly, the fourth hypothesis was accepted.

The dimensions of the digital incident response situational test were then examined.

Table 18 Posttest Differences between the Two Groups across the Dimensions of the Digital Incident Response Situational Test

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Initial verification and prioritization	6.84	0.91	5.08	0.83	10.10	< .001	2.02
Incident containment and impact reduction	6.68	0.77	5.08	0.60	11.61	< .001	2.32
Evidence preservation and initial documentation	7.34	0.59	6.28	0.64	8.59	< .001	1.72
Escalation and secure communication	6.20	0.61	4.64	0.69	11.98	< .001	2.40
Initial recovery and prevention of recurrence	6.40	0.83	5.06	0.59	9.30	< .001	1.86

The results in Table 18 show that the high-realism group achieved higher scores across all dimensions of digital incident response decision-making. The largest effect appeared in escalation and secure communication, followed by incident containment and impact reduction. This finding is important because responding to a digital incident requires more than recognizing a threat; it requires selecting a safe and procedurally appropriate action.

Fifth Hypothesis

The fifth hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the digital incident

response performance assessment rubric within the digital simulation environment, in favor of the high-realism scenario group.

Table 19 Independent-Samples t-Test for Posttest Differences in the Digital Incident Response Performance Rubric

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	102.70	4.86	41.432	< .001	8.29
Low-realism	50	69.46	2.92			

Table 19 shows a statistically significant posttest difference between the two groups in practical digital incident response performance, in favor of the high-realism scenario group. The effect size was extremely large, Cohen's d = 8.29. This value should be read cautiously because the instrument assessed procedural behaviors that were repeatedly practiced during the treatment. The high-realism scenarios required students to perform response actions, preserve evidence, document incidents, and communicate securely within contextually rich situations. Therefore, the large effect is most appropriately interpreted as evidence of strong treatment-performance alignment. This result indicates that the high-realism scenarios had a particularly strong effect on students' ability to perform response procedures inside the simulation environment.

ANCOVA was then conducted.

Table 20 ANCOVA Results for the Effect of Treatment on Digital Incident Response Performance

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	1692.432	< .001	0.946

Table 20 shows that the effect of the experimental treatment remained statistically significant after controlling for pretest scores, F = 1692.432, p < .001. The partial eta squared value was 0.946, indicating a very strong treatment effect. Accordingly, the fifth hypothesis was accepted.

The dimensions of the response performance rubric were also analyzed

.

Table 21 Posttest Differences between the Two Groups across the Dimensions of the Digital Incident Response Performance Rubric

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Initial verification and prioritization	21.70	1.59	14.74	0.80	27.57	< .001	5.51
Incident containment and impact reduction	25.78	1.53	17.42	0.95	32.84	< .001	6.57
Evidence preservation and practical documentation	22.62	1.03	14.70	0.86	41.72	< .001	8.34
Escalation and secure communication	19.68	0.51	13.46	0.71	50.41	< .001	10.08
Initial recovery and prevention of recurrence	12.92	0.92	9.14	0.50	25.53	< .001	5.11

Table 21 indicates that the high-realism group outperformed the low-realism group in all dimensions of practical digital incident response. The strongest difference appeared in escalation and secure communication, followed by evidence preservation and practical documentation. This suggests that high-realism scenarios were particularly effective in developing procedural response skills that depend on context, evidence, and role-appropriate decision-making.

Sixth Hypothesis

The sixth hypothesis stated that there would be a statistically significant difference at the .05 level between the mean post-test scores of students in the two experimental groups on the interaction analysis log within the digital simulation environment, in favor of the high-realism scenario group.

Because a statistically significant pretest difference had been found in the interaction analysis log in favor of the low-realism group, the posttest results were interpreted with particular attention to ANCOVA.

Table 22 Independent-Samples t-Test for Posttest Differences in the Interaction Analysis Log

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	71.06	3.75	34.879	< .001	6.98
Low-realism	50	50.50	1.81			

Table 22 shows a statistically significant posttest difference between the two groups in the interaction analysis log, in favor of the high-realism scenario group. Cohen's d was 6.98, indicating an extremely large effect.

Because the interaction analysis log captured behavioral traces within the simulation environment, this effect size reflects differences in the quality of students' actual interaction pathways, not only their final achievement scores. It should therefore be interpreted alongside the ANCOVA result, which controlled for the pretest difference in the interaction log.

To control for the pretest difference, ANCOVA was conducted.

Table 23 ANCOVA Results for the Effect of Treatment on the Interaction Analysis Log

Source of Variance	F	p	Partial Eta Squared
Experimental treatment	1182.646	< .001	0.924

Table 23 shows that the effect of the experimental treatment remained strongly significant after controlling for the pretest score, $F = 1182.646$, $p < .001$. The partial eta squared value was 0.924. Thus, the superiority of the high-realism group in interaction quality cannot be attributed to the initial pretest difference. Rather, it reflects the effect of the experimental treatment. Accordingly, the sixth hypothesis was accepted.

This result is especially important because the interaction analysis log did not measure final scores only. It captured how students performed inside the simulation environment: how they inspected evidence, how accurately they detected threats, how they responded to incidents, how efficiently they performed, and whether they acted independently and safely.

The dimensions of the interaction analysis log were also examined.

Table 24 Posttest Differences between the Two Groups across the Dimensions of the Interaction Analysis Log

Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Pattern of digital evidence inspection	14.08	0.90	9.76	0.52	29.43	< .001	5.89
Accuracy of threat detection	14.48	0.84	10.06	0.51	31.81	< .001	6.36
Quality of incident response	14.10	0.74	9.92	0.57	31.86	< .001	6.37
Performance and time efficiency	13.60	0.78	10.12	0.52	26.18	< .001	5.24
Independence, safe behavior, and documentation	14.80	0.81	10.64	0.48	31.21	< .001	6.24

Table 24 shows that the high-realism group outperformed the low-realism group across all dimensions of the interaction analysis log. The largest effects appeared in incident response quality, threat detection accuracy, and independence, safe behavior, and documentation. This pattern confirms that scenario realism influenced not only what students knew or selected in tests, but also how they behaved while interacting with the simulation environment.

Seventh Hypothesis

The seventh hypothesis stated that there would be a statistically significant difference at the .05 level between the mean scores of students in the two experimental groups on the perceived cyber-threat scenario realism scale, in favor of the high-realism scenario group.

This hypothesis was used as a manipulation check to verify that students actually perceived the difference in realism between the two treatments.

Table 25 Independent-Samples t-Test for Differences in Perceived Scenario Realism

Group	N	Mean	SD	t	p	Cohen's d
High-realism	50	132.66	8.75	32.755	< .001	6.55
Low-realism	50	87.26	4.42			

Table 25 shows a statistically significant difference between the two groups in perceived scenario realism, in favor of the high-realism group. The effect size was extremely large, Cohen's $d = 6.55$. This confirms that students did not merely receive two treatments that were theoretically different; they also perceived the high-realism scenarios as more realistic than the low-realism scenarios.

The dimensions of the perceived scenario realism scale were also examined.

Table 26 Differences between the Two Groups across the Dimensions of the Perceived Scenario Realism Scale

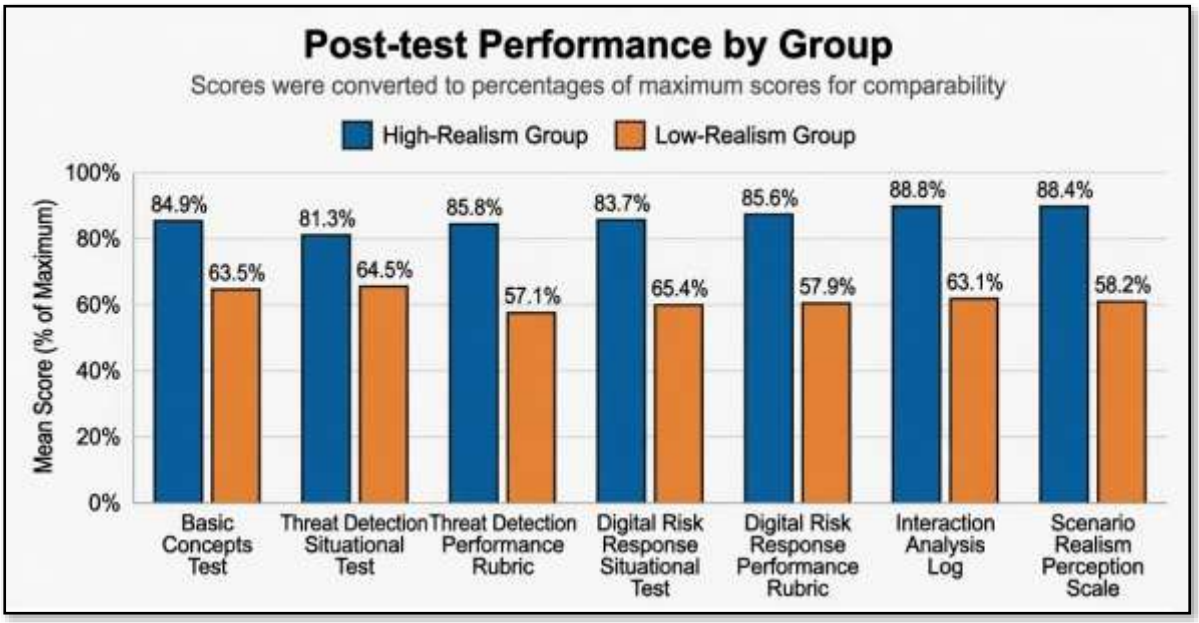
Dimension	High-Realism Mean	High-Realism SD	Low-Realism Mean	Low-Realism SD	t	p	Cohen's d
Realism of threat context	22.24	1.57	14.48	0.93	30.03	< .001	6.01
Realism of evidence and indicators	26.36	1.69	17.04	0.92	34.25	< .001	6.85
Realism of incident sequence	22.34	1.42	14.50	0.81	33.81	< .001	6.76
Realism of inspection and response tools	22.36	1.19	14.30	0.71	41.14	< .001	8.23
Realism of time pressure and decision consequences	22.92	1.28	14.90	0.81	37.48	< .001	7.50
Realism of ambiguity and decision-making	16.44	1.90	12.04	0.64	15.55	< .001	3.11

The results in Table 26 show that students in the high-realism group perceived the scenarios as more realistic across all dimensions. The strongest difference appeared in the realism of inspection and response tools, followed by the realism of time pressure and decision consequences, and the realism of evidence and indicators. This strengthens the internal validity of the study because it confirms that the experimental manipulation was clear and meaningful to students.

Accordingly, the seventh hypothesis was accepted.

To provide a comparable visual synthesis of post-test performance across instruments with different maximum scores, the mean scores for each instrument were converted into percentages of their respective maximum scores. Figure 7 presents the post-test performance of both groups across all research instruments.

Figure 7 Post-test Performance by Group



Note. Scores were converted to percentages of maximum scores to allow fair visual comparison across instruments with different maximum scores. Higher values indicate stronger post-test performance.

Figure 7 shows that the high-realism scenario group outperformed the low-realism scenario group across all post-measurement instruments. This superiority was not limited to a single outcome. Rather, it extended to conceptual knowledge, threat detection decisions, incident response decisions, practical performance, interaction quality, and perceived scenario realism. This pattern supports the consistency of the treatment effect across multiple sources of evidence.

Eighth Hypothesis

The eighth hypothesis stated that the high-realism scenario group would achieve greater gain than the low-realism scenario group across the research instruments measuring cyber-threat detection and digital incident response.

To test this hypothesis, gain scores were calculated by subtracting the pretest score from the posttest score for each student on each instrument. Independent-samples

t-tests were then used to compare the gain scores of the two groups.

Table 27 Differences between the Two Groups in Gain Scores across the Research Instruments

Instrument	High-Realism Gain Mean	High-Realism Gain SD	Low-Realism Gain Mean	Low-Realism Gain SD	t	p	Cohen's d
Core concepts test	13.30	4.12	4.86	2.24	12.721	< .001	2.54
Cyber-threat detection situational test	13.74	4.43	5.60	5.41	8.232	< .001	1.65
Performance observation rubric for cyber-threat detection	56.04	8.00	20.54	7.09	23.497	< .001	4.70
Digital incident response situational test	14.28	4.18	6.18	4.47	9.358	< .001	1.87
Digital incident response performance assessment rubric	55.12	6.81	20.98	6.62	25.417	< .001	5.08
Interaction analysis log	32.76	5.60	10.64	3.17	24.297	< .001	4.86

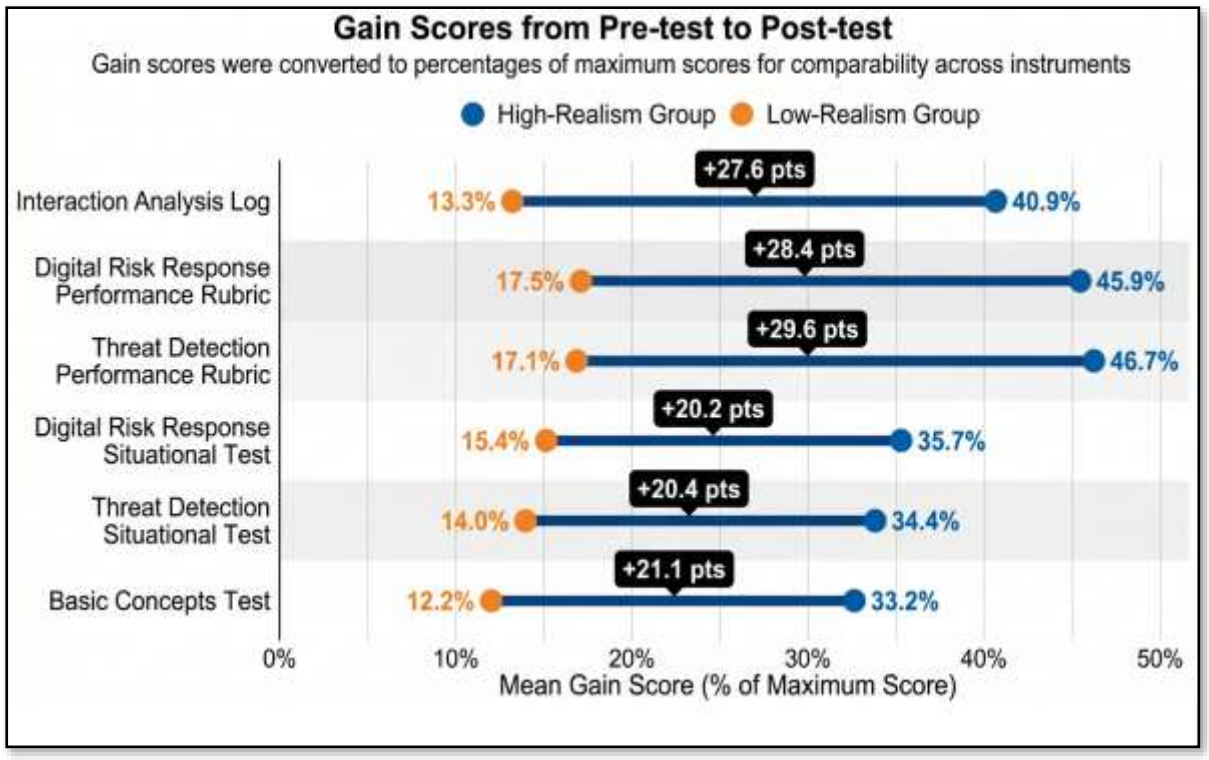
Table 27 shows that the high-realism scenario group achieved greater gain than the low-realism scenario group across all research instruments. The largest gain differences appeared in the digital incident response performance assessment rubric, the interaction analysis log, and the performance observation rubric for cyber-threat detection.

This pattern indicates that the added value of high realism was most evident in practical performance and behavioral interaction within the simulation environment. Although high-realism scenarios also improved conceptual knowledge and situational decision-making, their strongest effect appeared when students were required to act, document, respond, and interact with simulated digital evidence.

Accordingly, the eighth hypothesis was accepted.

To further clarify the developmental change from pretest to posttest, gain scores were visually summarized for both groups. Figure 8 presents the mean gain scores as percentages of each instrument's maximum score, making it possible to compare improvement across instruments with different scoring ranges.

Figure 8 Gain Scores from Pre-test to Post-test



Note. Points represent mean gain as a percentage of each instrument's maximum score; connecting lines show the gain advantage of the high-realism group.

Figure 8 shows that the high-realism scenario group achieved greater gain than the low-realism scenario group across all research instruments. The gap was especially evident in the practical performance rubrics and the interaction analysis log, indicating that high-realism scenarios had their strongest effect on applied and behavioral dimensions rather than on conceptual improvement alone. This pattern reinforces the interpretation that the treatment effect was not limited to post-test performance, but was also reflected in the amount of growth achieved during the experiment.

Summary of Hypothesis Testing

Table 28 Summary of Hypothesis Testing Results

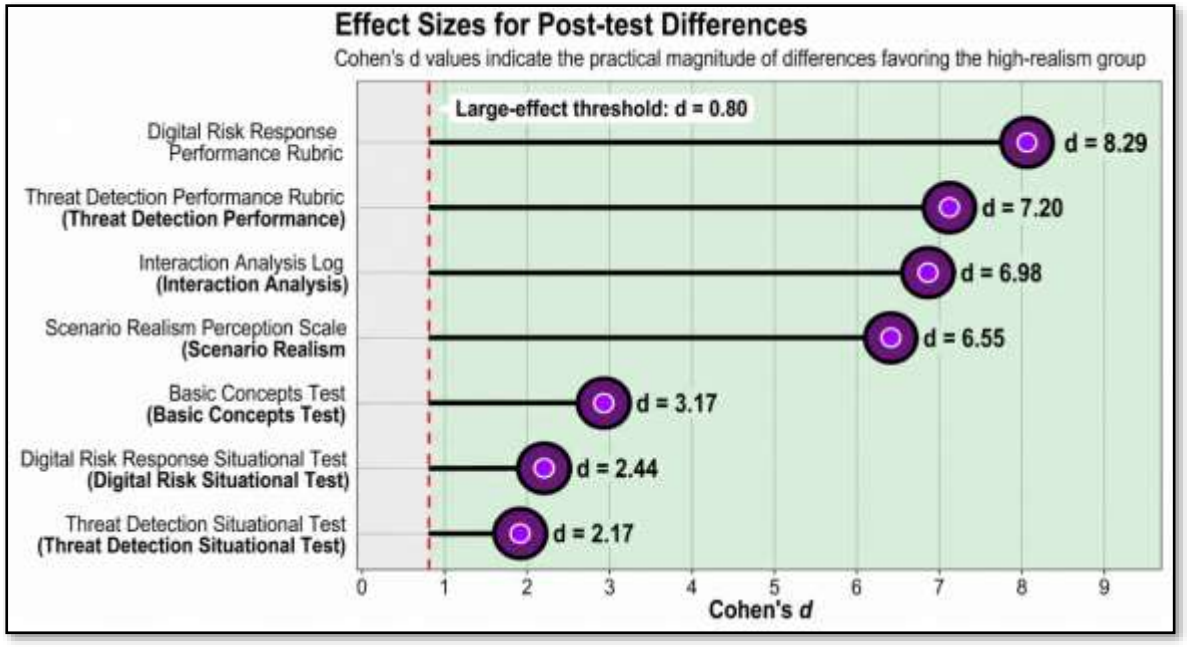
Hypothesis	Instrument or Indicator	Direction of Result	Decision
First hypothesis	Core concepts test	In favor of high-realism scenarios	Accepted
Second hypothesis	Cyber-threat detection situational test	In favor of high-realism scenarios	Accepted
Third hypothesis	Performance observation rubric for cyber-threat detection	In favor of high-realism scenarios	Accepted
Fourth hypothesis	Digital incident response situational test	In favor of high-realism scenarios	Accepted
Fifth hypothesis	Digital incident response performance assessment rubric	In favor of high-realism scenarios	Accepted
Sixth hypothesis	Interaction analysis log	In favor of high-realism scenarios after controlling for pretest scores	Accepted
Seventh hypothesis	Perceived scenario realism scale	In favor of high-realism scenarios	Accepted
Eighth hypothesis	Gain scores across research instruments	In favor of high-realism scenarios	Accepted

Table 28 shows that all research hypotheses were accepted. The results were consistent in one direction: students who learned through high-realism cyber-threat scenarios outperformed those who learned through low-realism scenarios in all dependent variables and in the manipulation-check measure.

Overall, the findings indicate that scenario realism was a powerful instructional design variable within the digital simulation environment. Its effect appeared not only in students' conceptual understanding but also in situational judgment, practical performance, digital incident response behavior, and quality of interaction within the simulation environment.

Beyond statistical significance, effect sizes were calculated to estimate the practical strength of the post-test differences between the two groups. Figure 9 presents Cohen's d values across the research instruments, with reference to the conventional threshold for a large effect.

Figure 9 Effect Sizes for Post-test Differences



Note. All reported effects exceeded the conventional large-effect threshold, indicating strong practical differences between groups. Higher values indicate stronger post-test advantage for the high-realism threat scenario treatment.

Figure 9 indicates that all effect sizes exceeded the conventional threshold for a large effect. This means that the differences between the two groups were not only statistically significant, but also practically meaningful. The largest effect sizes appeared in the performance rubrics and the interaction analysis log, which is expected given the direct alignment between these instruments and the nature of the experimental treatment based on practicing detection and response within simulated digital scenarios.

These very large effect sizes should be interpreted with methodological caution. They do not stand alone as the sole evidence of treatment effectiveness. Rather, they should be understood in relation to the consistency of results across multiple instruments, the use of pretest adjustment through ANCOVA, the direct alignment between the performance rubrics and the practiced scenario-based tasks, and the relatively low variability within the posttest performance scores. The convergence of cognitive, situational, performance-based, behavioral, and manipulation-check evidence provides a stronger basis for interpreting the treatment effect than any single effect-size estimate.

Discussion

Overview

The results of the study showed a consistent pattern of superiority for the high-realism scenario group over the low-realism scenario group across all post-measurement instruments. This superiority appeared in conceptual knowledge, situated decision-making, practical performance, interaction behavior, and perceived realism. The high-realism group also achieved greater gain scores from pretest to posttest across all dependent variables.

These findings should not be interpreted as isolated numerical differences. Rather, they represent an integrated pattern indicating that the realism level of cyber-threat scenarios within the digital simulation environment played a meaningful role in shaping the quality of students' learning. High-realism scenarios did not only help students remember concepts; they helped them use knowledge in context, inspect evidence, estimate risk, select safer responses, document decisions, and interact more effectively with simulated digital incidents.

This interpretation is consistent with the theoretical assumption underlying the study: cyber-threat detection and digital incident response are not purely cognitive skills. They are situated and performance-based skills that require learners to read a digital situation, connect multiple indicators, make a justified judgment, and respond safely under conditions that may involve uncertainty. Consequently, the stronger results of the high-realism group can be understood as an outcome of the closer alignment between the learning experience and the nature of the target skills.

Discussion of the Results of the Core Concepts Test

The first finding showed that students in the high-realism scenario group significantly outperformed students in the low-realism scenario group on the core concepts test. This indicates that high-realism scenarios supported not only practical performance but also conceptual understanding. Although the test measured knowledge, this knowledge was not presented to students as detached definitions. It was embedded in meaningful situations that required students to connect concepts such as phishing, impersonation, credential theft, unsafe sharing permissions, evidence preservation, escalation, and initial recovery to concrete educational digital contexts.

This result can be explained by the fact that high-realism scenarios made conceptual knowledge functional. Students did not learn cybersecurity terms as isolated information; they encountered these concepts while inspecting messages, reviewing links, analyzing file permissions, reading activity logs, and deciding whether a situation represented a threat. This form of contextualized learning likely strengthened the connection between concept and use. A student who learns "phishing" through a realistic Moodle-like message, a suspicious sender address, a misleading link, and an urgent request is more likely to understand the concept deeply than a student who reads a direct definition or identifies an obvious example.

The dimensional results of the core concepts test support this interpretation. The largest differences appeared in initial response procedures, incident classification and severity estimation, threat detection indicators, and documentation, escalation, and evidence preservation. These dimensions are closely connected to practical cybersecurity behavior. Therefore, the results suggest that high-realism scenarios strengthened the conceptual elements most needed for actual performance, rather than improving superficial recall only.

This finding aligns with simulation-based learning literature, which indicates that simulation is most effective when it connects knowledge to active decision-making and feedback (Chernikova et al., 2020). It also aligns with the logic of the NICE Framework, which represents cybersecurity competence as a combination of knowledge, skills, and tasks rather than as theoretical knowledge alone (Petersen et al., 2020).

Discussion of the Results of the Cyber-Threat Detection Situational Test

The second finding showed that the high-realism group significantly outperformed the low-realism group on the cyber-threat detection situational test. This result is central to the study because the situational test did not measure students' memorization of definitions. It measured their ability to use knowledge in suspicious digital educational situations.

The superiority of the high-realism group can be explained by the nature of the scenarios they experienced. High-realism scenarios trained students to read a digital situation as a set of interrelated evidence, not as a single obvious sign. In these scenarios, students

could encounter a sender address, a link, message wording, timing, an activity log, sharing permissions, and sometimes an attachment or alert. This type of situation required students to build their judgment by connecting evidence. It therefore resembled more closely the nature of cyber threats in real educational digital environments.

By contrast, low-realism scenarios, although they addressed the same skills, presented indicators more directly and with less ambiguity. Such scenarios may help students recognize a threat when it is obvious, but they may not train them to the same extent to deal with ambiguous situations or distributed indicators. This explains why the largest effect in the situational test appeared in severity estimation and distinguishing between genuine and false alerts. This dimension requires deeper judgment than merely naming a threat. It requires students to decide whether the available evidence is sufficient, whether the threat is serious, and what level of attention the situation deserves.

This result is consistent with research on phishing and social engineering, which shows that users often make unsafe decisions when they rely on surface features or trust familiar-looking messages without inspecting subtle indicators (Williams et al., 2018). It is also consistent with anti-phishing training literature, which suggests that applied and simulated training can improve users' ability to detect deceptive indicators during practice (Jampen et al., 2020).

Discussion of the Results of the Cyber-Threat Detection Performance Rubric

The third finding showed very large differences in favor of the high-realism group on the performance observation rubric for cyber-threat detection within the digital simulation environment. This finding is one of the strongest indicators of the effectiveness of the high-realism treatment because the rubric measured what students actually did while interacting with simulated threats.

The high-realism group outperformed the low-realism group across all performance dimensions: inspecting scenario elements and collecting evidence, analyzing suspicious indicators, identifying the threat type, estimating severity, and documenting the detection decision. The strongest effects appeared in documenting the detection decision and identifying the threat type. This suggests that high-realism scenarios helped students move beyond intuitive recognition toward evidence-based judgment.

The magnitude of the effect sizes in this instrument can be understood in light of the nature of the treatment and the assessment tool. High-realism scenarios required students to practice the same behaviors that were later assessed by the performance rubric. Students had to inspect evidence, connect indicators, justify decisions, and document their reasoning. Therefore, the assessment was sensitive to the practical difference between the two treatments. The low-realism group also practiced the target skills, but within simpler situations that demanded less evidence integration and less procedural documentation.

This result reinforces the idea that cybersecurity learning for non-specialist students should not be limited to awareness messages or conceptual instruction. A student may know that suspicious links are dangerous, but practical detection requires a different level of performance: checking the sender, previewing the link, reviewing the context, noticing inconsistencies, estimating severity, and documenting the judgment. High-realism scenarios provided a richer environment for practicing this full sequence.

The result also aligns with cybersecurity simulation literature, which emphasizes that scenario design determines the nature of trainee behavior, decision points, and assessment indicators (Yamin et al., 2020). When the scenario is realistic enough to require evidence-based performance, it becomes a bridge between knowledge and action.

Discussion of the Results of the Digital Incident Response Situational Test

The fourth finding showed that the high-realism group significantly outperformed the low-realism group on the digital incident response situational test. This indicates that the effect of scenario realism extended beyond threat detection to the next and equally important stage: choosing the appropriate response.

This result is important because many digital errors occur not only at the moment of detection but also at the moment of response. A student may recognize that a message is suspicious but delete it before preserving evidence. Another may realize that a link is dangerous but forward it to peers as a warning. A student may notice that a file is publicly accessible but remain unsure whether to change permissions, report the issue, document the incident, or do all of these in a particular sequence. Digital incident response therefore requires prioritization, awareness of decision consequences, and understanding of the student's role within the educational digital environment.

High-realism scenarios helped students practice this kind of thinking because they did not present the incident as an isolated event. Instead, they represented it as a situation with consequences, continuity, and follow-up decisions. When students saw that leaving a file publicly accessible could continue exposing data, or that deleting a message could result in the loss of evidence, they learned the meaning of safe response through the consequences of action.

The dimensional results support this interpretation. The largest effects appeared in escalation and secure communication, followed by incident containment and impact reduction. These are not simple recognition skills. They require students to understand what should be done, what should be avoided, who should be informed, and how communication can occur without widening the impact of the incident.

This result is consistent with contemporary cybersecurity frameworks that treat response as an essential function alongside detection and protection (NIST, 2018, 2024). It also supports the instructional decision to treat digital incident response as an independent target skill rather than assuming that it develops automatically after threat detection.

Discussion of the Results of the Digital Incident Response Performance Rubric

The fifth finding showed very large differences in favor of the high-realism group on the digital incident response performance assessment rubric. This result provides strong evidence for the effectiveness of the high-realism treatment because the rubric measured students' practical behavior when responding to simulated digital incidents.

The high-realism group outperformed the low-realism group across all response dimensions: initial verification and prioritization, incident containment and impact reduction, evidence preservation and practical documentation, escalation and secure communication, and initial recovery and prevention of recurrence. The strongest effect appeared in escalation and secure communication, followed by evidence preservation and practical documentation. This indicates that high-realism scenarios were particularly effective in developing skills that require procedural organization and institutional judgment, not merely individual awareness.

This can be explained by the fact that high-realism scenarios made students see that a digital incident is not a private or isolated situation. It may involve peer data, platform permissions, institutional accounts, technical support, or course administration. As a result, escalation and secure communication became a natural part of the response pathway rather than an additional instruction added after the event.

The high-realism scenarios also made documentation meaningful. Students documented because the scenario required justification, evidence preservation, and follow-up action. In low-realism scenarios, documentation could appear as a short written requirement after an obvious decision. In high-realism scenarios, however, documentation functioned as part of the response itself. This difference likely contributed to the strong effect found in evidence preservation and practical documentation.

This finding supports the argument that incident response training should be practiced through realistic procedural situations. Response skills cannot be fully developed by asking students to select a correct answer from a list. Students need to experience how one action affects the next, how evidence may be lost, how risk may spread, and how communication can either reduce or increase harm.

Discussion of the Results of the Interaction Analysis Log

The sixth finding showed that the high-realism group significantly outperformed the low-realism group on the interaction analysis log. This result is especially important because the interaction log did not measure final scores only. It captured the process of student behavior within the simulation environment: how students inspected evidence, how accurately they detected threats, how they responded to incidents, how efficiently they performed, and whether they acted independently and safely.

A pretest difference had appeared in the interaction analysis log in favor of the low-realism group. However, ANCOVA showed that the posttest difference remained strongly significant after controlling for the pretest score. This strengthens the interpretation that the superiority of the high-realism group was due to the experimental treatment rather than to initial differences between the two groups.

The superiority of the high-realism group in interaction quality can be explained by the richer demands imposed by high-realism scenarios. These scenarios required students to move among multiple evidence sources, compare indicators, delay judgment until evidence was inspected, document decisions, and select responses with consequences. This type of interaction naturally produces more meaningful behavioral traces than direct scenarios, where the student may identify the answer quickly without engaging deeply with the situation.

The largest effects in the interaction log appeared in incident response quality, threat detection accuracy, and independence, safe behavior, and documentation. This pattern confirms that scenario realism influenced the way students acted inside the environment, not merely their test scores. It also supports the value of learning analytics and interaction logs in evaluating simulation-based learning. In environments that aim to develop performance and decision-making, the process through which the learner reaches a decision may be as important as the final answer.

This result aligns with learning analytics literature, which emphasizes that digital interaction records can provide insight into learner behavior, learning pathways, and engagement patterns beyond final achievement scores (Ifenthaler & Yau, 2020). In the present study, the interaction log helped reveal that high-realism scenarios shaped the behavioral quality of learning.

Discussion of the Results of the Perceived Scenario Realism Scale

The seventh finding showed that students in the high-realism group perceived the scenarios as significantly more realistic than students in the low-realism group. This result is methodologically important because it confirms the validity of the experimental manipulation. The difference between the two treatments did not exist only in the researcher's design plan; it was also recognized by students during their learning experience.

The perceived realism scale covered several dimensions: realism of threat context, realism of evidence and indicators, realism of incident sequence, realism of inspection and response tools, realism of time pressure and decision consequences, and realism of ambiguity and decision-making. The high-realism group achieved higher scores across all these dimensions. The strongest differences appeared in the realism of inspection and response tools, realism of time pressure and decision consequences, and realism of evidence and indicators.

This finding reinforces the interpretation of the main results. If students had not perceived a meaningful

difference in realism between the two treatments, it would have been difficult to attribute differences in performance to scenario realism. The manipulation-check results therefore support the internal validity of the study and confirm that scenario realism was present in the learners' actual experience, not only in the researcher's theoretical classification.

At the same time, perceived realism should not be treated as a substitute for performance evidence. Its value lies in verifying the treatment, while the main educational effect is shown through the tests, performance rubrics, gain scores, and interaction log. The convergence of perceived realism results with performance and behavioral results strengthens the overall conclusion that high-realism scenarios produced a more powerful learning experience.

Discussion of Gain Scores from Pretest to Posttest

The eighth finding showed that the high-realism scenario group achieved greater gain than the low-realism scenario group across all research instruments. This result is important because it does not simply compare students' final levels. It measures the amount of improvement that occurred from pretest to posttest.

The gain was especially strong in the performance rubrics and interaction analysis log. This confirms that high realism had its strongest effect on practical and behavioral dimensions. This is logical because students in the high-realism group practiced the target performance within richer and more authentic situations. They therefore had more opportunity to grow in evidence inspection, indicator analysis, decision documentation, response execution, and interaction management within the environment.

The gain-score results also confirm that the posttest differences were not merely reflections of individual differences among students. Rather, they indicate that the high-realism group experienced greater development during the experimental period. This interpretation is further supported by the ANCOVA results, which showed that the treatment effect remained significant after controlling for pretest scores.

Taken together, the gain-score results suggest that high-realism scenarios were especially effective in moving students from general awareness to situated performance. The treatment did not simply raise scores at the end of the experiment; it produced a stronger developmental trajectory across the learning period.

Integrated Interpretation of the Findings

The findings of the present study can be interpreted through four interrelated explanations.

First, high-realism scenarios increased the authenticity of learning. Students encountered situations that resembled the digital environments they actually use, including Moodle, institutional email, cloud storage, shared files, activity logs, and incident documentation forms. This contextual proximity likely supported transfer from learning to practice.

Second, high-realism scenarios required evidence integration. Students could not rely on one obvious sign. They had to connect sender identity, link structure, message wording, access permissions, activity logs, and decision consequences. This process strengthened analytical judgment and reduced the likelihood of superficial recognition.

Third, high-realism scenarios connected decisions to consequences. Students saw how unsafe action could lead to continued exposure, evidence loss, expanded risk, or weak incident reporting. This helped them understand response as a procedural and ethical responsibility rather than as a single correct answer.

Fourth, high-realism scenarios required documentation and justification. Students had to explain why they classified a situation as a threat, what evidence supported their judgment, and what response was appropriate. This moved learning from guessing to accountable decision-making.

These explanations clarify why the differences were stronger in performance and behavioral instruments than in cognitive instruments. Knowledge can improve through both high- and low-realism training, but performance requires practice in situations that resemble real action. Thus, it was expected that the largest effects would appear in the performance rubrics and interaction analysis log.

The result of the perceived realism scale also supports the integrity of this interpretation. It shows that students recognized the difference between the two experimental treatments. In studies that examine realism as an instructional design variable, it is essential to verify that realism was experienced by learners and not assumed by the researcher only.

Overall, the results provide convergent evidence that high realism in cyber-threat scenarios helped move students from general cybersecurity knowledge to practical performance based on evidence inspection, risk estimation, and safe incident response within an educational digital simulation environment.

At the same time, the findings should not be interpreted as evidence that increasing realism is always beneficial in every simulation-based learning context. The results support the value of structured instructional realism, where additional details are directly related to the target skills and remain within learners' processing capacity. Uncontrolled realism, excessive complexity, or irrelevant detail may increase cognitive load and weaken learning. Thus, the contribution of the present study lies in showing the value of designed realism, not realism as mere complexity.

Main Conclusions

The study reached the following conclusions:

1. Cyber-threat scenario realism is an influential instructional design variable in digital simulation environments.
2. High-realism scenarios are more effective than low-realism scenarios in developing core concepts related to cyber-threat detection and digital incident response.
3. High-realism scenarios are more capable of developing cyber-threat detection skills because they present situations involving multiple pieces of evidence, appropriate

ambiguity, and the need to analyze interrelated indicators.

4. The effect of high-realism scenarios appears more strongly in practical performance than in theoretical knowledge because such scenarios require students to practice inspection, documentation, and response within situations close to real digital practice.
5. Digital incident response requires intentional and independent training because it does not develop automatically once students learn to detect threats.
6. The interaction analysis log is a valuable instrument for evaluating digital simulation environments because it reveals the pathway of performance within the environment, not only the final score.
7. The perceived scenario realism scale is necessary for verifying the validity of the experimental manipulation in studies that treat realism as an independent instructional design variable.
8. Controlling the platform, content, time, and assessment instruments across the two groups helped isolate the effect of scenario realism level and made the interpretation of the findings more consistent with the experimental design.

Recommendations

In light of the findings of the present study, the following recommendations are proposed:

1. Educational cybersecurity skills should be integrated into Educational Technology preparation programs. These skills should include cyber-threat detection, initial digital incident response, evidence preservation, documentation, and safe escalation.
2. Short instructional units should be embedded within Educational Technology courses to address digital threats related to learning platforms, institutional email, cloud storage, virtual meetings, and file-sharing permissions.
3. Safe digital simulation environments should be used to train Educational Technology students in dealing with cyber threats, rather than relying only on theoretical lectures or general awareness guidelines.
4. Scenario realism should be carefully considered when designing digital simulation environments. Scenarios should include multiple pieces of evidence, a logical incident sequence, appropriate ambiguity, and clear consequences for learner decisions.
5. Digital threats should not always be presented in an overly simplified or direct form, because such training may be insufficient for preparing students to deal with more ambiguous real-world situations.
6. Documentation and escalation should be taught as integral components of digital incident response, not as administrative procedures that occur after the response has already been completed.
7. Multiple assessment tools should be used when evaluating educational cybersecurity skills. These tools should cover knowledge, situational judgment, practical performance, interaction logs, and learners' perception of the treatment.
8. Interaction logs within digital learning environments should be used to analyze students' behavior during training, including evidence inspection patterns, response pathways, safe behavior, and documentation practices, rather than relying only on final test scores.
9. Faculty members and teaching assistants in Educational Technology programs should be prepared to design safe and pedagogically appropriate cyber-threat scenarios, while strictly avoiding the use of real malicious links, infected files, or offensive cybersecurity practices.
10. Educational institutions should develop procedural guides that help students respond appropriately to suspicious messages, untrusted links, data leakage, and unsafe file-sharing permissions.

Suggestions for Future Research

In light of the findings and delimitations of the present study, future research may address the following topics:

1. The effect of feedback timing within cyber-threat scenarios, immediate versus delayed feedback, on developing digital incident response skills among Educational Technology students.
2. The effect of cyber-threat scenario complexity, simple versus compound scenarios, on developing risk estimation skills and the ability to distinguish between genuine and false alerts.
3. A comparison between Moodle-based digital simulation and more specialized cybersecurity training environments in developing educational cybersecurity skills among university students.
4. The effect of work mode within the simulation environment, individual versus collaborative, on developing cyber-threat detection and digital incident response skills.
5. A qualitative study of Educational Technology students' thinking pathways while inspecting digital evidence within high-realism cyber-threat scenarios.
6. The effect of integrating learning analytics with digital simulation environments to provide remedial interventions for students who show unsafe digital behavior.
7. The effect of high-realism cyber-threat scenarios on developing digital security awareness among students from

specializations other than Educational Technology.

8. The development of an instructional design model for educational cybersecurity scenarios based on realism, safety, measurability, and learner appropriateness.
9. The effect of varying the threat source within the scenario, such as learning platform, institutional email, cloud storage, or virtual meeting, on developing threat detection skills among Educational Technology students.
10. The relationship between perceived scenario realism and cognitive and performance engagement within digital simulation environments.

Generalizability of the Findings

The findings of the present study should be interpreted within its methodological, human, and applied boundaries. The study was conducted with second-level students enrolled in the Department of Educational Technology at the Faculty of Specific Education during the first semester of the 2022/2023 academic year. Therefore, the generalization of the findings should be limited to students who are broadly similar in specialization, academic level, and prior digital learning experience.

The study was also implemented within a safe educational simulation environment rather than a specialized cyber range. Accordingly, the findings relate to basic defensive educational cybersecurity skills appropriate for Educational Technology students. They should not be generalized directly to advanced technical cybersecurity skills, such as network analysis, digital forensics, penetration testing, or organizational-level cyber incident management.

The scenarios used in the present study focused on threats associated with digital learning environments, including phishing, suspicious links, unsafe sharing permissions, data leakage, unusual login records, documentation, and escalation. Generalizing the findings to other types of digital threats requires further research.

Moreover, the study compared two levels of scenario realism within one digital simulation environment while controlling the platform, instructional content, learning time, and research instruments. Therefore, the findings should be understood within the boundaries of this design. They do not imply that increasing realism is always beneficial. Realism should be instructional, structured, and directly connected to the learning objective. Adding excessive detail may increase cognitive load and reduce learning value if the added details are not relevant to the target skill.

Limitations

Although the results of the present study were strong and consistent, several limitations should be acknowledged.

First, the study was conducted with one sample of Educational Technology students in a specific university context and within one academic semester. The scenarios were designed to suit the students' academic level and specialization; therefore, they did not include advanced technical cybersecurity skills.

Second, the digital simulation environment relied on safe and familiar educational tools, such as Moodle, interactive activities, and documentation forms. It did not use a professional cybersecurity training environment. This was an intentional design decision consistent with the educational aim of the study, but it limits the scope of generalization.

Third, practical performance was assessed through observation and performance assessment rubrics. Although these instruments were supported by validity, reliability, and inter-rater agreement indicators, their use remains dependent on the quality of rater training and the accuracy with which rating criteria are applied.

Fourth, the study measured the effect of scenario realism at the end of the experimental treatment. It did not examine the retention of learning after a delayed period or the transfer of skills to new digital educational situations. Future studies should therefore examine long-term retention and transfer of cyber-threat detection and digital incident response skills.

Conclusion

The present study examined the effect of cyber-threat scenario realism level, high-realism versus low-realism, within a digital simulation environment on developing cyber-threat detection and digital incident response skills among Educational Technology students. The study was grounded in a clear educational need: preparing Educational Technology students to face digital incidents that may appear in learning environments, not as cybersecurity specialists, but as users, designers, and supporters of educational digital systems that require defensive awareness and safe behavior.

The findings showed that high-realism scenarios were more effective than low-realism scenarios in developing knowledge, decision-making, practical performance, interaction quality, and perceived realism. These findings indicate that the scenario within a simulation environment is not merely a narrative frame for activity. It is a central instructional design element that shapes how students think, perform, and respond. The closer the scenario is to the structure of a real educational digital situation, in terms of evidence, ambiguity, sequence, consequences, and documentation, the greater its ability to move learning from the level of knowledge to the level of performance.

The study therefore offers an important implication for Educational Technology: educational cybersecurity can be taught and practiced appropriately when it is designed as safe, realistic, and instructionally structured scenarios. Developing secure digital behavior cannot be achieved through general awareness alone. It requires simulation-based situations in which students inspect, decide, document, and respond. Accordingly, integrating this type of experience into Educational Technology preparation programs is no longer an optional addition. It is becoming a necessary component of the quality and safety of digital learning environments.

Funding
This research received no external funding.

Conflict of Interest
The authors declare that they have no conflict of interest.

Data Availability Statement
The datasets generated and analyzed during the current study are not publicly available due to participant privacy and confidentiality considerations, but aggregated results may be made available from the corresponding author upon reasonable request.

Author Contributions
Tamer M. Kamel contributed to the study conception, research design, development of the digital simulation environment, data collection, statistical analysis, and drafting of the manuscript. Mahmoud N. Rashwan contributed to reviewing the theoretical framework, research instruments, and methodological procedures. Mohamed W. Soliman contributed to reviewing the instructional treatment, validating the research instruments, and revising the manuscript. All authors reviewed and approved the final version of the manuscript.

References

1. Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), 62–68. https://doi.org/10.1109/TALE.2018.8615162
2. Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, 185–197. https://doi.org/10.1016/j.chb.2016.02.065
3. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://arxiv.org/abs/1901.02672
4. Brynielsson, J., & Franke, U. (2014). Cyber situational awareness: A systematic review of the literature. Computers & Security, 46, 18–31. https://doi.org/10.1016/j.cose.2014.06.008
5. Chernikova, O., Heitzmann, N., Stadler, M., Holzberger, D., Seidel, T., & Fischer, F. (2020). Simulation-based learning in higher education: A meta-analysis. Review of Educational Research, 90(4), 499–541. https://doi.org/10.3102/0034654320933544
6. Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale. Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2873–2882. Association for Computing Machinery. https://doi.org/10.1145/2702123.2702249
7. Gegenfurtner, A., Quesada-Pallarès, C., & Knogler, M. (2020). Digital simulation-based training: A meta-analysis. British Journal of Educational Technology, 51(6), 2191–2210. https://doi.org/10.1111/bjet.13009
8. Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), Article e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
9. Herrington, J., & Oliver, R. (2000). An instructional design framework for authentic learning environments. Educational Technology Research and Development, 48(3), 23–48. https://doi.org/10.1007/BF02319856
10. Huang, W., Hew, K. F., & Lo, C. K. (2019). Investigating the effectiveness of gamification in learning: A meta-analysis. Educational Technology Research and Development, 67, 1333–1360. https://doi.org/10.1007/s11423-019-09670-w
11. Ifenthaler, D., & Yau, J. Y.-K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. Educational Technology Research and Development, 68, 1961–1990. https://doi.org/10.1007/s11423-020-09788-z
12. Issenberg, S. B., McGaghie, W. C., Petrusa, E. R., Lee Gordon, D., & Scalese, R. J. (2005). Features and uses of high-fidelity medical simulations that lead to effective learning: A BEME systematic review. Medical Teacher, 27(1), 10–28. https://doi.org/10.1080/01421590500046924
13. Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. Human-centric Computing and Information Sciences, 10, Article 33. https://doi.org/10.1186/s13673-020-00237-7
14. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: State of the art and future directions. Journal of Cybersecurity, 7(1), Article tyab005. https://doi.org/10.1093/cybsec/tyab005
15. Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Prentice-Hall.
16. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 905–914. Association for Computing Machinery. https://doi.org/10.1145/1240624.1240760
17. Lateef, F. (2010). Simulation-based learning: Just like the real thing. Journal of Emergencies, Trauma, and Shock, 3(4), 348–352. https://doi.org/10.4103/0974-2700.70743
18. Lave, J., & Wenger, E. (1991). Situated learning: Legitimate peripheral participation. Cambridge University Press.

19. Mangaroska, K., & Giannakos, M. (2019). Learning analytics for learning design: A systematic literature review of analytics-driven design to enhance learning. IEEE Transactions on Learning Technologies, 12(4), 516–534. https://doi.org/10.1109/TLT.2018.2868673
20. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. Computers in Human Behavior, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065
21. Merrill, M. D. (2002). First principles of instruction. Educational Technology Research and Development, 50(3), 43–59. https://doi.org/10.1007/BF02505024
22. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. https://doi.org/10.6028/NIST.CSWP.04162018
23. National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. National Institute of Standards and Technology.
24. Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3
25. Paas, F., & van Merriënboer, J. J. G. (2020). Cognitive-load theory: Methods to manage working memory load in the learning of complex tasks. Current Directions in Psychological Science, 29(4), 394–398. https://doi.org/10.1177/0963721420922183
26. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire: Two studies of information security awareness. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.007
27. Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29
28. Petersen, R., Santos, D., Wetzel, K., Smith, M. C., & Witte, G. (2020). Workforce framework for cybersecurity (NICE Framework) (NIST Special Publication 800-181 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1
29. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382. Association for Computing Machinery. https://doi.org/10.1145/1753326.1753383
30. Siemens, G. (2013). Learning analytics: The emergence of a discipline. American Behavioral Scientist, 57(10), 1380–1400. https://doi.org/10.1177/0002764213498851
31. Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. https://doi.org/10.1207/s15516709cog1202_4
32. Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2020). A review of cyber-ranges and test-beds: Current and future trends. Sensors, 20(24), Article 7148. https://doi.org/10.3390/s20247148
33. Viberg, O., Hatakka, M., Bälter, O., & Mavroudi, A. (2018). The current landscape of learning analytics in higher education. Computers in Human Behavior, 89, 98–110. https://doi.org/10.1016/j.chb.2018.07.027
34. Vlachopoulos, D., & Makri, A. (2017). The effect of games and simulations on higher education: A systematic literature review. International Journal of Educational Technology in Higher Education, 14, Article 22. https://doi.org/10.1186/s41239-017-0062-1
35. Willems, C., Pitropakis, N., Buchanan, W. J., & Tsikerdekis, M. (2022). The cyber security body of knowledge and curricula development for cyber security education. Education and Information Technologies, 27, 6835–6863. https://doi.org/10.1007/s10639-022-10877-8
36. Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. International Journal of Human-Computer Studies, 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004
37. Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, Article 101636. https://doi.org/10.1016/j.cose.2019.101636