Measuring Change – Evaluating Cybersecurity Awareness Before and After a Video-Based Learning Module

Alexander Lawall*, Ulrike Plach†, Birdal Güvendi†, Kilian Stöckle†
*IU International University of Applied Sciences
Erfurt, Thüringen, Germany
alexander.lawall@iu.org
†OTH Regensburg
Regensburg, Bavaria, Germany
ulrike.plach@oth-regensburg.de, birdal.güvendi@extern.oth-regensburg.de, kilian.stoeckle@st.oth-regensburg.de

***Abstract*—Cybersecurity awareness among students in non-technical degree programs is often insufficient, despite their extensive use of digital services in everyday life. This study addresses the challenge of improving cybersecurity awareness and self-reported behavior in higher education through low threshold digital learning interventions. The objective is to evaluate whether a video-based learning module can measurably influence students' awareness, attitudes, and behaviors related to cybersecurity. A pre/post study design was applied using two nearly identical standardized questionnaires administered before and after the intervention to answer the research questions. The study involved 104 first-semester undergraduate students who participated in a learning unit consisting of four instructional videos covering core cybersecurity topics. The results indicate that approximately 77% of participants had no prior cybersecurity training, confirming a low baseline level. Descriptive analyses show small but consistent improvements in cybersecurity awareness and selected behavioral indicators, particularly in phishing recognition and online shopping security. However, statistical testing revealed no significant overall differences between pre/post-test results. In conclusion, the findings suggest that video-based learning is effective as an introductory and sensitizing approach for cybersecurity education, but insufficient on its own to produce immediate, significant behavioral change. Future educational designs should therefore combine video-based content with interactive, practice-oriented, and longitudinal learning elements to foster sustained cybersecurity behavior in higher education.**

***Keywords*-Cybersecurity awareness; video-based learning; higher education; phishing; online shopping security; mobile security; digital behavior change.**

I. Introduction

This section introduces the motivation, research objectives, and overall contribution of the study. It outlines the problem context, formulates the research questions, and positions the work within the broader field of cybersecurity education.

A. Motivation and Background

In an increasingly digitalized world, cybersecurity has become a critical concern. For young adults who interact daily with digital devices and online services, a fundamental understanding of security measures is essential. Higher education institutions face the challenge of not only delivering subject-specific knowledge but also fostering security awareness among their students. At OTH Regensburg, the degree programs Digital Business Management and International Business Management include the course "Digital Technology Skills" in the first semester. As part of this learning unit, a dedicated activity called the Cybersecurity Challenge is conducted to strengthen students practical understanding of cybersecurity.

B. Research Objectives and Questions

The course Digital Technology Skills combine in-class sessions with an online learning platform where students engage with instructional videos outside the lecture. As part of the Cybersecurity Challenge, students were required to watch four videos addressing key topics in cybersecurity, including password security, phishing awareness, online shopping, safe browsing practices, and data protection.

The primary objective of this paper is to examine the impact of this digital learning intervention on students attitudes and behaviors regarding cybersecurity. Specifically, the study aims to:

1) Assess students existing knowledge and practices related to cybersecurity prior to the learning unit.
2) Identify changes in awareness, attitudes, and self-reported behaviors after completing the video-based learning activities.

To achieve these objectives, two standardized questionnaires were administered:

- Part I (Pre-test): Captured baseline knowledge and behavior before the learning unit.
- Part II (Post-test): Conducted after students watched the videos to identify potential changes.

The findings presented in this paper seek to answer the following research questions:

RQ1: What was the initial level of cybersecurity awareness among students?
RQ2: To what extent did the digital learning intervention influence their attitudes and behaviors?

C. Contribution and Structure

The findings of this study aim to provide insights into the effectiveness of digital learning formats in promoting cybersecurity awareness and encouraging tangible behavioral changes among students. By analyzing pre/post intervention

data, this paper contributes to the ongoing discussion on how learning approaches can support higher education institutions in addressing cybersecurity challenges.

The remainder of the paper is structured as follows. Section II reviews related work on cybersecurity awareness and digital learning interventions. Section III outlines the conceptual foundation of the video-based learning module. Section IV describes the pre/post study design and data analysis. Section V presents the empirical findings and discusses implications for cybersecurity education. Section VI concludes with a summary and outlook for future work.

II. Related Work

This section reviews relevant literature on cybersecurity awareness in higher education, the effects of digital learning interventions, and the role of video-based and blended learning approaches. It establishes the theoretical and empirical foundation for the present study.

A. Baseline Cybersecurity Awareness in Higher Education

Prior research consistently shows that higher education students enter university with insufficient cybersecurity awareness, particularly regarding phishing, password security, and digital privacy [1]. Large-scale surveys reveal that approximately 30–40% of students cannot correctly identify phishing attempts [2] [3]. Simulated attack studies show high susceptibility, with 67.67% of participants disclosing sensitive information during a WhatsApp-based social engineering simulation [4]; similar behavioral susceptibility has also been observed in academic-community phishing studies [5]. Similarly, assessments using established metrics, such as the Digital Competence Framework for Educators (DigCompEdu) framework, find that 93.5% of students demonstrate only intermediate digital security competence, and just 0.6% reach high competence levels [6].

Baseline misconceptions appear across multiple domains. Students routinely overestimate their ability to identify cyber threats [2] [7], yet fail to label risky scenarios as dangerous [8]. Only certain subpopulations, such as IT majors, show comparatively higher initial preparedness, though even these groups often lack secure habitual behaviors [9]. Collectively, these findings indicate that most university students begin with moderate theoretical knowledge but weak practical behavioral competence, highlighting the need for pedagogically structured interventions that target both cognition and behavior [10].

B. Effects of Digital Learning Interventions on Cybersecurity Attitudes and Behaviors

1) Knowledge Gains: Across studies, digital learning interventions consistently produce substantial improvements in cybersecurity knowledge. Effect sizes ranging from Cohen's $d = 0.81$ to $d = 1.50$ are common in gamified, video-based, and modular e-learning approaches [11] [12]. Even short interventions, such as a 20-minute educational game, yield 50–67% increases in phishing-related knowledge [13].

Gamification is among the most frequently used strategies and has been shown to significantly improve knowledge in areas, such as password management, internet use, and information handling [14]. However, these gains do not always generalize to behavioral intentions or compliance attitudes, indicating a gap between knowing and doing.

2) Behavioral and Attitudinal Change: While knowledge gains are robust, behavioral change is more challenging to achieve. Interventions that rely solely on information dissemination, such as quizzes or passive video consumption, tend to improve cognitive awareness but have limited impact on real-world behavior.

The most successful interventions incorporate:

- repeated practice,
- self-efficacy development,
- simulated or authentic threat exposure,
- reflection or debriefing cycles.

For example, competence-based training using progressive exposure to phishing simulations reduced student vulnerability from 67.67% to 1.67%, ultimately reaching 0% after repeated rounds [4]. Protection Motivation Theory (PMT) grounded studies similarly show that self-efficacy strongly predicts behavioral intention, suggesting that interventions should deliberately cultivate confidence in performing secure behaviors [15].

Overall, the literature indicates that, while digital learning reliably improves cybersecurity knowledge, behavioral and attitudinal change requires specific pedagogical design rather than content delivery alone.

C. Effectiveness of Video-Based Learning Approaches

Blended learning, which integrates digital content with instructor-led components, has emerged as a highly effective approach, particularly for non-technical student populations. Studies employing blended designs consistently show:

- larger effect sizes than stand-alone digital modules,
- better translation of knowledge to applied behavior,
- improved student motivation and engagement.

For example, blended programs incorporating gamification, classroom discussion, and hands-on application demonstrate statistically significant, domain-wide improvements in cyber hygiene behaviors [16]. Even low cost or freemium platforms, such as Kahoot! modules, show strong results when embedded in instructor supported environments [17].

At the same time, research highlights an important caveat: single-session interventions produce short-term gains but are susceptible to decay unless reinforced through spaced repetition [12]. This has direct implications for video-based learning modules, which are often used in short, stand-alone formats. Evidence suggests that such modules are most effective when combined with additional learning activities, such as quizzes, guided practice, or reflection tasks, to strengthen retention and promote behavioral transfer.

D. Synthesis and Implications for the Present Study

The reviewed literature converges on three key insights that directly align with the research questions of this study:

1) *Initial awareness levels.* Initial cybersecurity awareness among higher education students is generally low to moderate, with substantial vulnerabilities in phishing recognition, password hygiene, and digital citizenship. Even when students demonstrate theoretical knowledge, their behavioral susceptibility remains high [2] [4] [6].
2) *Impact of digital interventions.* Digital learning interventions reliably improve cybersecurity knowledge, often with large effect sizes. However, the translation of knowledge into attitudes and secure behaviors depends on factors, such as self-efficacy, practice opportunities, and reinforcement mechanisms. Short video-based modules excel in knowledge transmission but may require supplementary elements to influence behavior [11] [14] [15].
3) *Role of blended learning.* Blended learning provides the strongest overall impact on cybersecurity competence, particularly for non-technical learners. Existing research indicates that blended formats enhance engagement, deepen understanding, and improve both cognitive and behavioral outcomes compared to digital-only approaches [12] [16] [17].

The present study contributes to this body of work by empirically evaluating the impact of a video-based learning module, examining not only knowledge gains but also attitudinal and behavioral indicators. In doing so, it extends prior findings by assessing whether a structured, video-centered intervention can meaningfully shift cybersecurity competence in higher education settings and provide evidence on how video-based learning may support lasting behavior change.

III. Intervention Design and Learning Content

This section presents the conceptual foundation of the video-based learning module examined in this study. The selected videos introduce fundamental cybersecurity concepts, highlight prevalent and emerging threats, and frame cybersecurity as a shared socio-technical responsibility rather than a purely technical concern. Collectively, the videos address cognitive, behavioral, and attitudinal dimensions of cybersecurity competence, which are particularly relevant for students in non-technical degree programs.

A. Video 1: Cybersecurity Fundamentals, Threat Landscape, and Shared Responsibility

The first video introduces cybersecurity as a broad socio-technical discipline concerned with protecting digital assets according to the core objectives of Confidentiality, Integrity, and Availability (CIA) triad, cf. [18]. This framework provides a foundational model for understanding cyber risks and appropriate protection measures across devices, applications, networks, cloud infrastructures, and emerging technologies, such as Internet of Things (IoT) systems. By highlighting the ubiquity of digital technology in everyday life, the video frames cybersecurity as a shared responsibility relevant to both private and professional contexts.

Cybersecurity is further conceptualized as a layered process comprising preventive, detective, and corrective controls, reflecting defense-in-depth principles. The video emphasizes the importance of understanding attacker behavior, attack vectors, and evolving threat methodologies to design effective defenses. Acknowledging that absolute security is unattainable, it introduces incident response and digital forensics as essential components for resilience. Emerging technologies, such as artificial intelligence, are discussed as dual-use factors that support both attacks and defenses. The video concludes by linking theoretical principles to basic cyber hygiene practices, reinforcing the role of informed user behavior in effective cybersecurity.

B. Video 2: Phishing Awareness and Safeguarding Information in Digital Interactions

The second video focuses on cybersecurity risks in online shopping, a common digital activity frequently associated with phishing, fraud, and data breaches, cf. [19]. It emphasizes the identification of trustworthy online shops through careful Uniform Resource Locator (URL) inspection, avoidance of suspicious links, and independent background research. These practices directly address common redirection and fake-shop attack scenarios.

The video introduces transport-layer security as a baseline requirement for protecting sensitive transaction data, highlighting Hypertext Transfer Protocol Secure (HTTPS) and encryption indicators as practical heuristics for non-technical users. It further distinguishes between data protection in transit and data protection at rest, emphasizing that secure storage practices can limit the impact of breaches. Convenience features, such as saving payment information, are framed as usability-security trade-offs, encouraging informed decision-making based on provider reputation, security maturity, and visible certifications. By briefly addressing provider-side responsibilities, the video reinforces the socio-technical nature of secure online transactions.

C. Video 3: Secure Online Shopping and Risk-Aware Transaction Behavior

The third video reiterates the core cybersecurity principles related to online shopping and serves as a reinforcement unit within the learning sequence, cf. [20]. From a pedagogical perspective, repetition supports retention and habit formation, which are critical for cybersecurity behaviors that rely on routine decision-making under time pressure.

Key practices, such as verifying website legitimacy, recognizing phishing indicators, and assessing encrypted communication, are restated to emphasize their role as default behaviors rather than exceptional precautions. The video again highlights the distinction between data protection in transit and at rest, and reiterates the shared responsibility between users and service providers. This reinforcement strengthens the likelihood that learners internalize secure behaviors and

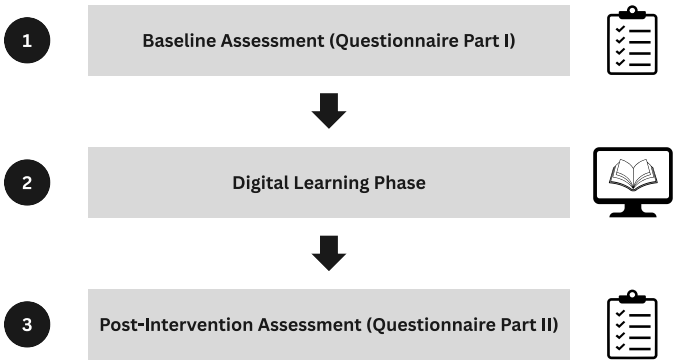

Figure 1. Process of the Cybersecurity Learning Unit.

apply them consistently, supporting the interpretation of post-intervention changes as emerging behavioral consolidation, rather than short-term effects.

D. Video 4: Smartphone Security and Privacy Protection in Mobile Environments

The fourth video addresses cybersecurity risks associated with smartphones, emphasizing that mobile devices are fully fledged computing platforms with comparable threat exposure to traditional computers, cf. [21]. It highlights the importance of regular operating system and application updates, as well as device lifecycle management, to mitigate known vulnerabilities.

Authentication mechanisms, such as PINs and biometric controls, are discussed as effective but limited safeguards that reduce, rather than eliminate, risk. The video examines mobile banking and multi-factor authentication, emphasizing the potential risk of combining authentication and service access on a single device and introducing the concept of factor separation. Platform-specific security assumptions are challenged by highlighting comparable vulnerabilities across mobile operating systems. Additional risks related to malicious applications, phishing, and public wireless networks are discussed, with Virtual Private Network (VPN) usage and situational awareness presented as mitigating strategies. Overall, the video frames mobile security as a combination of technical safeguards and risk-aware user behavior.

IV. Methodology

The learning unit on cybersecurity consisted of three sequential steps, as illustrated in Figure 1. Baseline Assessment (Questionnaire Part I): Students completed an initial questionnaire comprising 27 questions based on [22] and designed to capture their existing knowledge and behaviors related to cybersecurity. The questionnaire included items assessing both knowledge and self-reported behavior. Example questions include:

- "Do you set a password for your phone?"
- "Do you set a password for your computer?"
- "Do you use a complex password?"

These items were measured using ordinal response scales to capture behavioral tendencies and awareness levels.

Digital Learning Phase: Participants then engaged with four instructional videos on cybersecurity topics. Post-Intervention Assessment (Questionnaire Part II): After viewing the videos, students completed a second questionnaire, which was nearly identical to the first. This follow-up survey included additional questions regarding their subjective perception of the learning content and any intended behavioral changes. Students generated a personal code word to link their responses across both questionnaires to ensure anonymity while enabling data pairing. Participation was voluntary and conducted under strict confidentiality. In addition, both questionnaires were completed online.

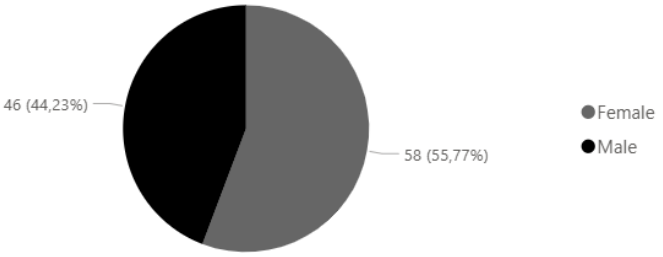

Figure 2. Distribution of Participants by Gender.

Critical Reflection: Several limitations should be considered when interpreting the results. First, the study relies on self-reported data, which may be subject to bias. Second, the short duration of the intervention limits the ability to observe long-term behavioral change. Third, the sample consists of first-semester students, which may restrict generalizability. Finally, the absence of a control group prevents causal attribution of observed changes solely to the intervention.

V. Results and Discussion

This section presents and interprets the empirical findings of the pre/post-intervention survey, focusing on changes in cybersecurity awareness, attitudes, and self-reported behaviors following the video-based learning module.

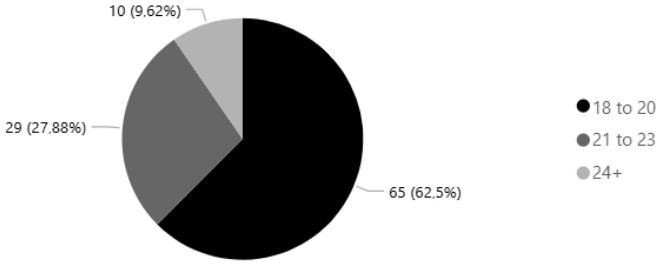

Figure 3. Age Group Distribution of Participants.

A. Sample Characteristics and Baseline Context

The study sample consisted of 104 first-semester students enrolled in business-oriented degree programs. As shown in Figure 2, the gender distribution was balanced, with 58 female (55.77%) and 46 male (44.23%) participants. Figure 3 indicates that most respondents were between 18 and 23 years of age, representing a cohort that is highly active in digital environments.

Baseline exposure to cybersecurity education was limited. As illustrated in Figure 4, 77.88% of participants reported no prior participation in cybersecurity workshops, confirming that the sample largely represents a novice population. This supports the relevance of the intervention and aligns with prior research indicating low to moderate baseline cybersecurity awareness among non-technical students.

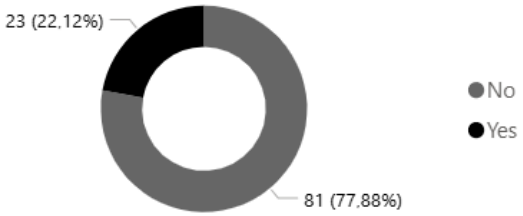

Figure 4. Self-Reported Prior Knowledge.

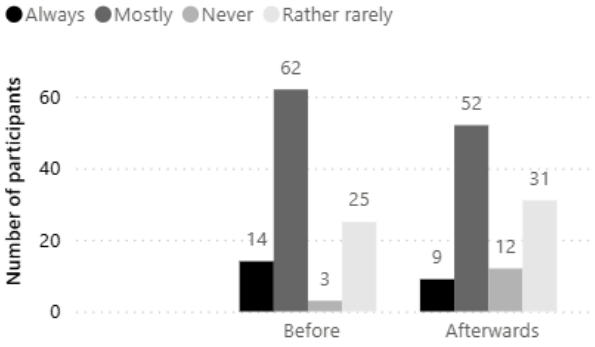

Figure 5. Password Change Awareness.

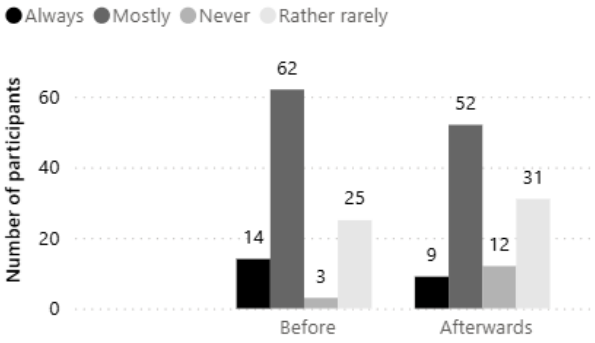

Figure 6. Phishing Awareness.

B. Changes in Awareness and Self-Reported Behavior

Figures 5 to 7 visualize pre/post-test responses for selected cybersecurity domains, including general awareness, password practices, and phishing recognition. Across most items, descriptive analysis shows small but consistent shifts toward more security-conscious responses following the learning module.

Password-related behavior, shown in Figure 5, reveals modest improvements. After the intervention, fewer students reported frequent re-use of the same password across multiple accounts, and a slight increase was observed in responses indicating safer password practices. While these changes are limited in magnitude, they point toward an emerging reflection on personal security habits.

The greatest observable improvement appears in phishing awareness. Figure 6 shows an increase in the number of students who reported knowing what phishing is, alongside a reduction in those who indicated uncertainty. This aligns with the targeted content of the videos on phishing, online shopping, and mobile security, and reflects findings from prior studies that phishing awareness is particularly responsive to short, focused educational interventions.

Figure 7 (Awareness) indicates an increase in self-reported cybersecurity awareness after the intervention, suggesting that the videos successfully heightened students perception of cybersecurity relevance. This effect is particularly important, as awareness is a prerequisite for subsequent behavioral change.

C. Statistical Analysis

Descriptive statistics show that mean values across questionnaire items ranged from 1.02 to 3.63 in the pre-test and from 1.00 to 3.77 in the post-test, with moderate standard deviations indicating heterogeneous baseline behaviors among students. Quartile distributions suggest that the majority of responses were already clustered in the moderately security-aware range before the intervention.

Correlation analysis yielded a very strong positive Pearson correlation between pre/post-test responses (r = 0.927), indicating high internal consistency and stability in students self-reported behavior patterns across both measurement points. This suggests that the intervention did not fundamentally alter underlying response structures but rather produced incremental shifts within an otherwise stable behavioral framework.

A paired-samples t-test comparing pre- and post-test mean values resulted in $t = 0.543$, $p = 0.616$, indicating no statistically significant difference at the conventional $\alpha = 0.05$ level. The corresponding effect size (Cohen's d) was small, suggesting that the intervention produced only minor changes at the aggregate level. Although statistical significance was not achieved, consistent directional trends across multiple indicators suggest a systematic, small intervention effect. Such patterns may indicate early-stage behavioral change processes that require reinforcement.

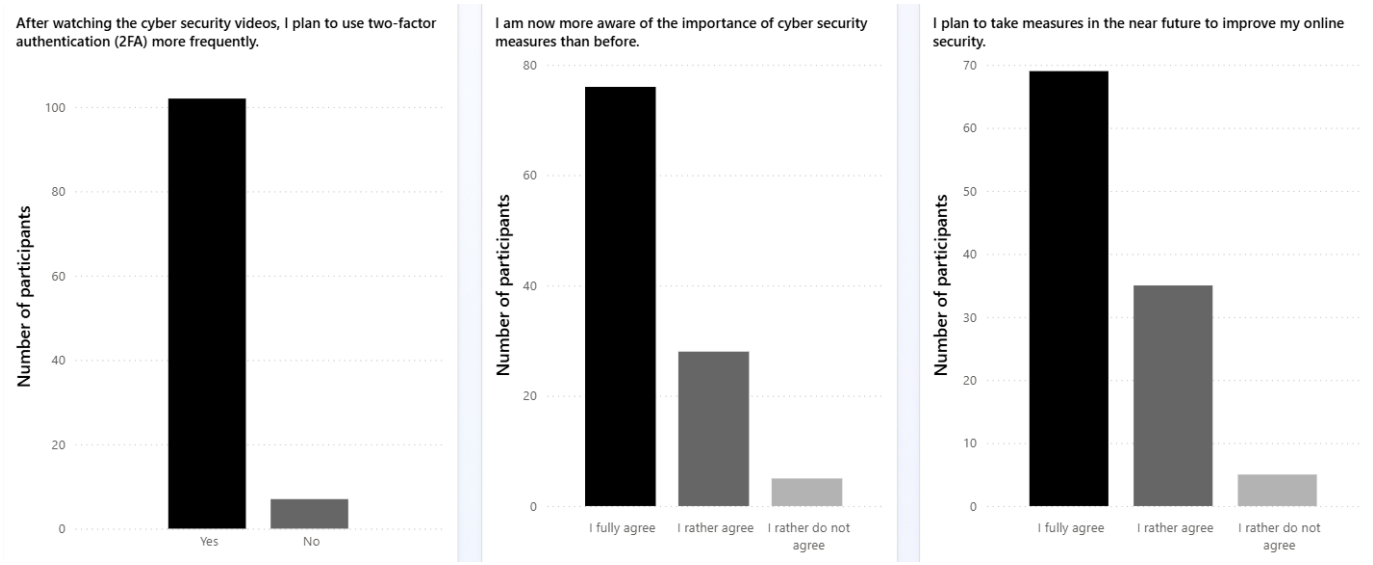

Figure 7. Self-Reported Post-test Participant Awareness.

D. Interpretation and Discussion

The absence of statistically significant differences does not imply that the intervention was ineffective. Instead, the results indicate that the video-based learning module primarily contributed to awareness raising and reflective adjustment, rather than immediate, large-scale behavioral transformation, cf. Figure 7. This interpretation is supported by the visual trends in Figures 5 to 7, which consistently show directional improvements despite limited effect sizes.

Generalizability and Theoretical Implications: Beyond cybersecurity education, the observed distinction between awareness gains and limited behavioral change reflects a broader phenomenon in digital learning and behavioral science. Informational interventions are often effective at increasing cognitive awareness. They are insufficient to trigger immediate behavioral change without reinforcement mechanisms. This aligns with established behavior change theories, such as Protection Motivation Theory, which emphasize the role of self-efficacy, repeated exposure, and contextual relevance. The concept of *reflective adjustment*, observed in this study, therefore represents an intermediate outcome between knowledge acquisition and sustained behavioral change. This intermediate stage may be critical for designing scalable educational interventions across domains, such as data privacy, digital health literacy, or sustainability education.

Several factors may explain these findings. First, the intervention was short and primarily informational, which prior research has shown to be more effective at improving knowledge and awareness than at producing immediate behavioral change. Second, cybersecurity behaviors, such as password management or cautious online decision-making, are habitual and context-dependent, often requiring repeated practice and reinforcement to change sustainably. Third, the strong correlation between pre-/post-test responses suggests that deeply ingrained habits are resistant to change through a single exposure.

Importantly, the results align with existing literature on video-based cybersecurity education, which consistently reports modest short-term behavioral effects but meaningful gains in awareness and risk perception. In this context, the observed improvements in phishing recognition and self-reported awareness represent valuable outcomes, particularly for first-semester, non-technical students.

Overall, the findings suggest that video-based learning modules are well-suited as introductory and sensitizing tools within a broader learning strategy. While they may not be sufficient on their own to produce statistically significant behavioral change, they provide a critical foundation upon which more interactive, practice-oriented, and longitudinal interventions can build.

VI. Conclusion and Future Work

This study investigated the effects of a video-based learning module on cybersecurity awareness and self-reported behavior among first-semester students in non-technical degree programs.

With respect to *RQ1*, the results confirm that students entered the course with limited prior exposure to formal cybersecurity education and only moderate baseline awareness. Although many participants reported familiarity with selected security concepts, the pre-test results revealed inconsistencies in secure everyday behaviors, particularly in areas, such as password re-use and online risk assessment. These findings align with prior research indicating that higher education students often overestimate their cybersecurity competence despite existing behavioral vulnerabilities.

Regarding *RQ2*, the pre/post comparison shows that the video-based intervention contributed to increased cybersecurity awareness and improved recognition of common threats, most notably phishing. While descriptive trends indicate small but consistent improvements in several behavioral indicators, the statistical analysis did not reveal significant overall changes. This suggests that the intervention primarily supported awareness raising and reflective engagement rather than immediate behavioral transformation.

Future work should therefore extend the observation period, integrate hands-on and scenario-based learning components, and account for individual baseline differences when evaluating intervention effects. Longitudinal studies could further examine whether repeated or scaffolded video-based interventions lead to measurable behavioral change over time. Overall, the results provide valuable guidance for designing effective cybersecurity awareness programs in higher education and highlight the importance of combining digital content with active learning strategies.

Additionally, future research should explore domain-specific adaptations of cybersecurity awareness interventions. Rather than addressing cybersecurity as a broad and abstract concept, targeted modules focusing on specific domains (e.g., healthcare, critical infrastructure, or finance) may increase relevance and behavioral transfer. Learners operating within a familiar domain context are more likely to connect educational content with real-world consequences. Thereby strengthening the transition from awareness to action. Such domain-specific approaches may also enable the transfer of lessons learned from prior incidents ("known bad outcomes") into actionable behavioral patterns within the learners' own professional or academic environments.

REFERENCES

[1] I. Adeshola and D. I. Oluwajana, "Assessing cybersecurity awareness among university students: implications for educational interventions," *Journal of Computers in Education*, vol. 12, no. 4, pp. 1283–1305, 2025.

[2] E. K. Perrault, "Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing," *Journal of Educational Computing Research*, vol. 55, no. 8, pp. 1154–1167, 2018.

[3] K. Okokpujie, M. A. Ariyo, F. S. Moninuola, M. B. Akanle, and I. P. Okokpujie, "Evaluating students' vulnerability and awareness to phishing attacks in educational institutions." *International Journal of Safety & Security Engineering*, vol. 15, no. 3, 2025.

[4] C. Azaabi, "Improving digital security and privacy of students in colleges of education: An attitudinal change framework based on competence learning matrix," *European Journal of Education Studies*, vol. 9, no. 10, 2022.

[5] A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia*, vol. 44, no. 1, pp. 53–67, 2020.

[6] N. Torres-Hernández, T. Pessoa, and M. J. Gallego-Arrufat, "Intervención y evaluación con tecnologías de la competencia en seguridad digital," *Digital education review*, pp. 111–129, 2019.

[7] A. K. Gwenhure, "University students' security behavior against email phishing attacks: insights from the health belief model," *Journal of Cybersecurity*, vol. 11, no. 1, p. tyaf034, 11 2025. [Online]. Available: https://doi.org/10.1093/cybsec/tyaf034

[8] Y. Rudenko, L. Sytnyk, R. Pasichnyi, O. Bieliaieva, N. Dehtiarova, and A. Barabash, "Analyzing the results of a study of the effectiveness of developing students' cybersecurity skills," in *2025 MIPRO 48th ICT and Electronics Convention*. IEEE, 2025, pp. 390–395.

[9] E. M. Katsika, "Simulation Based Learning in Critical Infrastructure Security Awareness: An Empirical Study," Ph.D. dissertation, University of Piraeus (Greece), 2020.

[10] A. Lawall, "Steigerung des Lernerfolgs der Studierenden durch digitale, interaktive Umfrage- und Feedbacksysteme [Enhancement of students' learning outcomes through digital, interactive survey and feedback systems]," *Hochschulmanagement*, vol. 17, no. 1/2, pp. 55–58, 2022.

[11] O. J. Mason, S. Collman, S. Kazamia, and I. Boureanu, "Preparing UK Students for the Workplace: The Acceptability of a Gamified Cybersecurity Training." *Journal of Cybersecurity Education, Research and Practice*, vol. 2024, no. 1, pp. 1–7, 2024.

[12] E. Kim, J. Kwon, J. Yoon, and A. M. Agogino, "Embedding cybersecurity into design education: Increasing designers' awareness of cybersecurity throughout the design process," in *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, vol. 59216. American Society of Mechanical Engineers, 2019, p. V003T04A008.

[13] P. Weanquoi, J. Johnson, and J. Zhang, "Using a game to improve phishing awareness," *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, no. 2, p. 2, 2018.

[14] T. Wu, K.-Y. Tien, W.-C. Hsu, and F.-H. Wen, "Assessing the effects of gamification on enhancing information security awareness knowledge," *Applied Sciences*, vol. 11, no. 19, p. 9266, 2021.

[15] N. F. Khan, N. Ikram, H. Murtaza, and M. Javed, "Evaluating protection motivation based cybersecurity awareness training on kirkpatrick's model," *Computers & Security*, vol. 125, p. 103049, 2023.

[16] M. A. Salem and A. E. E. Sobaih, "A quadruple "e" approach for effective cyber-hygiene behaviour and attitude toward online learning among higher-education students in saudi arabia amid covid-19 pandemic," *Electronics*, vol. 12, no. 10, p. 2268, 2023.

[17] R. Matovu, J. C. Nwokeji, T. Holmes, and T. Rahman, "Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges," in *2022 IEEE frontiers in education conference (FIE)*. IEEE, 2022, pp. 1–9.

[18] A. Lawall. (2023) Cyber Security: Tips and Trends. [retrieved: November, 2025]. [Online]. Available: https://www.youtube.com/watch?v=utsZF1qOo68

[19] ——. (2023) Phishing: Types and Tips About Safeguarding Your Information. [retrieved: November, 2025]. [Online]. Available: https://www.youtube.com/watch?v=7Bm9TeZ7kNg

[20] ——. (2023) Online Shopping Safety. [retrieved: November, 2025]. [Online]. Available: https://www.youtube.com/watch?v=9VUHXORDVCI

[21] ——. (2023) Smartphone Security: How to Protect Your Phone Privacy. [retrieved: November, 2025]. [Online]. Available: https://www.youtube.com/watch?v=66XwzE9qdFs

[22] I. A. Zahid, S. A. Hussein, and S. M. Mahdi, "Measuring individuals cybersecurity awareness based on demographic features," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 20, no. 1, pp. 58–67, 2024.