2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #52428

Building Cybersecurity Awareness Through an Introductory Course for Non-Technical Students

Prof. Gary D Steffen, Purdue University Fort Wayne

Gary Steffen is Director of the School of Polytechnic at Purdue University Fort Wayne(PFW).

Building Cybersecurity Awareness Through an Introductory Course for Non-Technical Students

This practice-oriented design case describes the development and delivery of an introductory cybersecurity course for non-technical undergraduate students. As cybersecurity risks increasingly affect personal, academic, and professional life, students across disciplines need opportunities to develop foundational cybersecurity awareness without requiring advanced technical preparation. Grounded in Kolb's experiential learning theory and supported by Bloom's Taxonomy, the course uses familiar digital behaviors, case studies, guided reflection, and applied assignments to help students connect cybersecurity concepts to everyday decision-making. The paper presents the course rationale, instructional design, sample learning activities, and lessons learned from implementation in a general education context. Preliminary observations from student reflections and classroom engagement suggest that students became more comfortable discussing cybersecurity risks, connecting security concepts to their academic and career interests, and recognizing cybersecurity as a shared responsibility across disciplines. The paper also identifies challenges related to balancing technical depth, supporting students with varied backgrounds, and delivering experiential activities across mixed modalities. The course offers a practical model for institutions seeking to broaden cybersecurity literacy through accessible, interdisciplinary general education coursework.

Introduction

Digital technology now fills nearly every aspect of daily life and professional practice, making cybersecurity an increasingly visible and consequential concern. Cybersecurity is no longer limited to protecting financial accounts or safeguarding a Social Security number. Instead, it touches nearly every domain in which individuals and organizations operate, from social media platforms and cloud-based collaboration tools to the companies that students will one day work for. Emerging issues such as data breaches, identity theft, and the growing prevalence of deepfake technologies further underscore the extent to which cybersecurity shapes personal, academic, and professional decision-making [1], [2].

Historically, higher education responded to technological change by emphasizing computer literacy. At one point, many colleges and universities required students to demonstrate proficiency in basic computing skills, including word processing, spreadsheet use, and presentation software. Over time, these requirements were reduced or eliminated as such skills became commonplace and were assumed to be acquired earlier in students' educational experiences. While this shift reflects changes in baseline technological familiarity, it has also created an unintended gap. Comfort with technology use does not necessarily translate into an understanding of cybersecurity risks, responsibilities, or best practices [2], [3].

As a result, cybersecurity awareness has become an essential competency that extends well beyond traditional computing or engineering disciplines. Students across all majors routinely interact with digital systems that store sensitive personal and organizational information. Yet many complete their academic programs with limited preparation to recognize risks, evaluate threats, or make informed decisions regarding information security. National and professional

guidance increasingly emphasizes the importance of cybersecurity education for diverse learner populations, highlighting the need for foundational cybersecurity literacy across disciplines [2].

This paper addresses that need through the design of *ITC 18000 – Introduction to Computer Security*, a three-credit course developed for students outside technical computing fields at Purdue University Fort Wayne. The course introduces foundational cybersecurity concepts that prioritize accessibility, relevance, and practical engagement. Rather than emphasizing technical implementation or programming skills, the course focuses on helping students understand cybersecurity principles as they relate to everyday digital practices, academic responsibilities, and future professional roles, consistent with broader cybersecurity education recommendations [2]. Unlike many introductory cybersecurity courses that rely on technical labs or system-level interaction, this course intentionally avoids device-specific requirements. Instead, it emphasizes conceptual understanding, reflection, and real-world application.

This paper presents a practice-oriented account of the development of ITC 18000, with particular attention to course design, instructional strategies, and pedagogical decision-making. Grounded in experiential learning theory [4], the paper describes how the course content was structured and delivered to make technical material accessible to non-technical students. This paper presents a practice-oriented design case describing the development and implementation of an introductory cybersecurity course for non-technical students within a general education context. While many institutions have introduced cybersecurity awareness courses, these efforts vary widely in their emphasis on technical depth, target audience, and instructional approach. This work contributes to this growing area by focusing specifically on non-technical students and by emphasizing experiential, reflection-based learning as a means of improving cybersecurity literacy. The paper also includes preliminary observations related to student engagement, interdisciplinary relevance, and instructional challenges encountered during course delivery.

Rationale and Context

The development of ITC 18000 – Introduction to Computer Security was motivated by a clear institutional need to make cybersecurity concepts accessible to students across all majors at Purdue University Fort Wayne. Rather than positioning cybersecurity as a specialized or exclusively technical domain, the course was intentionally designed to introduce security principles to any student interested in understanding how digital systems shape personal, academic, and professional environments. This inclusive approach reflects the reality that cybersecurity risks and responsibilities extend well beyond traditional computing fields.

The course is available to students through the university's general education curriculum as part of the Interdisciplinary Ways of Knowing requirement. This category emphasizes the development of a broad understanding across multiple disciplines and encourages students to analyze complex issues from diverse perspectives. Courses approved in this area are expected to support learning outcomes related to interdisciplinary analysis, synthesis, ethical reasoning, and the integration of ideas across academic fields. Cybersecurity aligns naturally with these goals, as security challenges frequently intersect with moral considerations, privacy concerns, global implications, and professional responsibility [7]. By situating ITC 18000 within this framework,

the course provides students with an opportunity to explore cybersecurity as an interdisciplinary issue rather than a purely technical problem [5].

In addition to fulfilling general education requirements, ITC 18000 serves as a foundational course within an interdisciplinary Cyber Security minor. The 15-credit minor is designed for non-technical majors and combines introductory information technology coursework with core cybersecurity concepts and policy-focused content. The minor intends to provide students from any discipline with a foundational understanding of cybersecurity principles that complement their primary field of study. Emphasis is placed on security fundamentals, risk awareness, and policy considerations rather than advanced technical implementation. The minor is open to all majors, except for degree programs in the Information Systems and Information Technology, reinforcing its focus on interdisciplinary participation and non-technical learners [6].

Designing a cybersecurity course for this audience also required careful consideration of student perceptions and attitudes toward technology. Many students are enthusiastic users of emerging technologies and are comfortable adopting new digital tools in their daily lives. They often enjoy discussing technology and sharing their experiences with peers. At the same time, a significant number of students express discomfort or intimidation when technology is framed as "technical" in nature. Students in non-technical majors may view themselves primarily as end users of technology. They may not initially recognize the importance of developing technical competence related to cybersecurity risks, vulnerabilities, and best practices. This perception can create barriers to engagement if cybersecurity content is presented in ways that reinforce a sense of technical intimidation rather than its relevance [3].

Alignment with institutional goals related to general education, interdisciplinary learning, and cybersecurity literacy was therefore central to the course design. By embedding cybersecurity education within existing general education and multidisciplinary structures, ITC 18000 reinforces the idea that cybersecurity awareness is a shared responsibility across disciplines. The course supports institutional efforts to prepare students for responsible participation in an increasingly digital society by emphasizing informed decision-making, ethical awareness, and an understanding of how cybersecurity principles apply within diverse academic and professional contexts [2], [5].

Theoretical Framework: Experiential Learning

The instructional design of *ITC 18000 – Introduction to Computer Security* is grounded in experiential learning, which emphasizes knowledge creation through experience, reflection, and application. Experiential learning theory, most notably articulated by Kolb, conceptualizes learning as a cyclical process involving concrete experience, reflective observation, abstract conceptualization, and active experimentation [8]. This framework served not only as a theoretical foundation but also as a practical design guide for developing a cybersecurity course intended for students without technical computing backgrounds.

Kolb's experiential learning model was intentionally used to shape both the course's structure and sequencing. Rather than organizing content around technical domains, tools, or systems, ITC 18000 was designed around learning experiences that move students through the stages of the

experiential learning cycle. This approach ensured that cybersecurity concepts were consistently introduced in ways that were accessible, relevant, and grounded in students' existing digital practices. For non-technical learners, this design choice was particularly important, as it reframed cybersecurity from a technical specialization into a set of informed decisions and responsibilities encountered in everyday life.

Course development began by identifying everyday digital experiences among students across disciplines, such as using social media platforms, cloud-based file storage, password management, and online collaboration tools. These experiences serve as concrete anchors for each instructional unit. Beginning with familiar contexts allows students to engage with cybersecurity concepts without the immediate barrier of technical terminology, reducing the intimidation factor while increasing relevance. Students are encouraged to recognize that cybersecurity is already embedded in their daily lives and behaviors, even if it is not always explicitly acknowledged.

Reflective observation is emphasized through guided discussions and structured reflective activities that prompt students to examine their assumptions about security, privacy, and risk. These reflections encourage students to consider how their digital habits may expose them to vulnerabilities or ethical concerns, and how those risks may vary across personal, academic, and professional contexts. Reflection also provides students with a space to articulate connections between cybersecurity issues and their chosen fields of study, reinforcing the course's interdisciplinary focus.

Abstract conceptualization is introduced after students have engaged with experience and reflection. Core cybersecurity principles, including risk, threats, vulnerabilities, access control, and policy considerations, are presented as interpretive tools for understanding the situations students have already examined. By sequencing instruction in this manner, abstract concepts are anchored in concrete examples, allowing students to develop conceptual clarity without becoming overwhelmed by technical detail. This approach supports deeper understanding while maintaining accessibility for learners who may not identify as technically inclined.

Active experimentation completes the experiential learning cycle by asking students to apply cybersecurity concepts to new and unfamiliar situations. Assignments and activities require students to analyze real-world scenarios, evaluate potential security risks, and propose informed responses grounded in course concepts. These applications may include case study analysis, evaluation of organizational security practices, or the development of personal or professional security strategies. Through active experimentation, students move beyond awareness toward informed action, reinforcing cybersecurity as a practical and transferable competency.

Table I summarizes how Kolb's experiential learning cycle was operationalized in the design of instructional activities for ITC 18000.

Table I
Alignment of Kolb's Experiential Learning Cycle with Course Design in ITC 18000

Kolb Learning Stage	Instructional Focus	Example Application in ITC 18000
Concrete Experience	Engage students through familiar digital behaviors	Examination of everyday activities such as social media use, password practices, cloud storage, and online collaboration
Reflective Observation	Encourage analysis of assumptions and behaviors.	Guided discussions and reflective prompts addressing privacy, risk, and responsibility in personal and academic contexts
Abstract Conceptualization	Introduce formal cybersecurity concepts.	Instruction on risk, threats, vulnerabilities, access control, and policy framed around prior experiences
Active Experimentation	Apply concepts to new situations.	Case study analysis, evaluation of cybersecurity incidents, and development of personal or organizational security strategies

The alignment presented in Table I is reinforced through specific course activities and assignments. For example, phishing analysis exercises and case-based discussions provide concrete experiences that introduce students to real-world cybersecurity scenarios. Reflective assignments prompt students to examine their own digital behaviors and assumptions about security and risk. Conceptual understanding is developed through structured instruction in foundational topics such as threats, vulnerabilities, and risk management, while application is emphasized through case-study analysis and the final research project. Together, these activities support movement through the experiential learning cycle and help students connect abstract cybersecurity concepts to practical, real-world contexts.

While Kolb's experiential learning model guided the structure and sequencing of instructional activities, Bloom's Taxonomy provides a complementary lens for understanding the cognitive levels targeted in the course [9], [10]. As an introductory, general education course, ITC 18000 emphasizes lower- to mid-level cognitive outcomes, particularly remembering and understanding foundational cybersecurity terminology and concepts, while extending into analysis and evaluation through reflective activities and case-based assignments. Memorization of key terms and definitions provides a necessary foundation that enables students to interpret, analyze, and evaluate cybersecurity scenarios relevant to their personal and professional lives. Higher-order creation is approached conceptually through synthesis and informed decision-making rather than technical system implementation, consistent with the course's non-technical focus.

Course Design

The design of ITC 18000 reflects an intentional progression from individual-level digital behaviors to broader organizational, ethical, and societal considerations in cybersecurity. Course content is structured to support non-technical learners by beginning with familiar contexts and

gradually introducing more complex concepts, while maintaining a consistent emphasis on reflection, case analysis, and informed decision-making rather than technical system manipulation. This sequencing aligns with the course's experiential learning framework and supports accessibility for students from diverse academic backgrounds.

The course begins with an introduction to foundational security concepts, including the need for information security and the drivers that influence cybersecurity decisions in modern organizations. Early modules focus on personal security, allowing students to examine cybersecurity through the lens of their own digital practices. Topics such as password management, personal devices, and online behavior are introduced before broader system-level discussions, enabling students to recognize cybersecurity as a lived experience rather than an abstract technical domain. This early emphasis establishes relevance and inclusion and lowers barriers to engagement for students who may not view their academic programs as technical in nature.

As the course progresses, attention shifts from individual practices to computer, internet, and mobile security. These modules introduce students to risks, threats, and vulnerabilities associated with commonly used technologies, while avoiding direct manipulation of hardware or system configurations. Because students' personal devices and technical skill levels vary widely, the course design intentionally avoids activities that require changes to system settings that may be difficult to reverse or could introduce unintended consequences. Instead, learning activities emphasize analyzing scenarios, evaluating case studies, and reflecting on best practices. This approach allows students to engage with cybersecurity concepts without requiring advanced technical proficiency or specialized equipment.

Reflection and case analysis are central components throughout the course. Weekly discussions and assignments prompt students to analyze real-world cybersecurity incidents, emerging technologies, and digital threats, encouraging them to apply course concepts to situations they may encounter as employees, managers, or personally. The required course textbook reinforces this approach by emphasizing practical cybersecurity awareness and application rather than technical configuration, further supporting the course's focus on conceptual understanding and everyday decision-making.

Later modules address privacy, ethics, and cybersecurity law, broadening the course's scope to include the societal and organizational dimensions of security. These topics encourage students to consider the ethical responsibilities, legal implications, and professional expectations associated with cybersecurity across disciplines. Rather than requiring students to engage directly with formal standards or regulatory frameworks, instruction emphasizes common terminology, ethical reasoning, and everyday actions that contribute to secure organizational practices. This structure supports the course's goal of preparing students to be informed and responsible participants in digitally mediated workplaces, even when formal standards may not be directly referenced in their professional roles.

The course concludes in an individual research project that allows students to explore a cybersecurity topic aligned with their interests and academic backgrounds. The project requires a

substantial research paper and professional presentation, emphasizing analysis, synthesis, and reflection rather than technical implementation. Evaluation criteria prioritize content knowledge, depth of analysis, research quality, and the ability to connect course concepts to real-world contexts, reinforcing the course's emphasis on interdisciplinary understanding and critical thinking.

Taken together, the course design and sequencing of ITC 18000 support a clear learning experience that balances conceptual rigor with accessibility. By organizing content around progressively complex cybersecurity contexts and relying on reflection and case-based analysis rather than system-level manipulation, the course enables non-technical students to develop meaningful cybersecurity literacy. This structure reinforces cybersecurity as a shared responsibility across disciplines and prepares students to engage thoughtfully with digital security challenges in their personal and professional lives.

Instructional Strategies and Learning Activities

Instructional strategies in ITC 18000 were designed to emphasize accessibility, relevance, and engagement for students from non-technical majors. From the outset, cybersecurity concepts are introduced through real-world examples that directly affect students' everyday lives. Rather than beginning with abstract technical models, instruction focuses on familiar contexts such as social media use, personal devices, online accounts, and widely reported cybersecurity incidents.

To accommodate students with widely varying levels of technical confidence, course topics and assignments were intentionally selected to be appropriate for any college-level learner. Mathematical content and advanced technical detail were removed or simplified, allowing students to focus on understanding concepts, terminology, and implications rather than implementation. This approach reinforces cybersecurity literacy as a foundational competency rather than a specialized technical skill set.

Accessibility across platforms was a central design consideration. Each assignment was reviewed carefully to ensure it could be completed without reliance on a specific operating system or hardware configuration. Because students enrolled in the course use a range of devices, including Windows and macOS systems, learning activities were designed to avoid system-level configuration changes that students might not be able to reverse. This decision also reflected a concern for student confidence and digital safety. Instead of requiring hands-on manipulation of personal systems, many activities rely on online resources, guided analysis, and reflective case studies. This approach allows all students to engage fully with the course material regardless of their technical environment.

Experiential and reflective learning are emphasized throughout the course. Instruction consistently focuses on personal digital behavior and how everyday actions connect to security outcomes. Course content frequently references typical applications used by college students and integrates current events. Reflection is treated as a substantive learning activity rather than an informal add-on. Students are asked to reflect explicitly on their assumptions, behaviors, and decision-making processes related to cybersecurity. These reflections are then used as inputs for

class discussions, allowing instructional emphasis to shift toward areas that may be underdeveloped or misunderstood.

Case studies serve as another key instructional strategy. Rather than emphasizing technical forensic analysis, case studies are used to encourage students to locate relevant information, evaluate sources, and reason through cybersecurity issues using available online resources. This approach reinforces critical thinking and information literacy while remaining aligned with the course's non-technical focus. Case analysis also supports movement through the experiential learning cycle by prompting students to apply concepts to situations beyond their own immediate experience.

The course's structure supports engagement across delivery modalities. Live lecture sessions are recorded and shared with online students, allowing them to experience the pacing and context of in-person instruction. During class sessions, recordings are paused to facilitate in-class exercises, and online students are prompted to complete comparable activities independently. This approach helps maintain consistency between course sections while preserving opportunities for experiential engagement.

Course assignments and discussions closely follow the textbook's structure, supplemented by current events and emerging cybersecurity issues. Homework assignments reinforce key concepts through application and reflection, while discussions provide opportunities for students to articulate their understanding and learn from peers. Quizzes and exams focus primarily on foundational knowledge and terminology, emphasizing recall and comprehension appropriate for an introductory course. These assessments are designed to support learning rather than serve as gatekeeping mechanisms.

The course culminates in an individual research project that allows students to pursue a cybersecurity topic of personal or professional interest. The project is intentionally individual rather than group-based to ensure that learning remains personal and reflective rather than distributed across team members. Students are encouraged to select topics that extend course concepts and emphasize analysis, ethical awareness, and real-world relevance rather than technical implementation. Through this project, students synthesize course learning and demonstrate their ability to engage thoughtfully with cybersecurity issues relevant to their lives and future careers.

Several instructional trade-offs were made intentionally in the design of ITC 18000. While simple technical experiments could have been incorporated, these were excluded due to concerns about unequal access to technology and the feasibility of consistent implementation across delivery formats. Instead, demonstrations of technical concepts are provided during class sessions and made available to online students through recordings. Students who wish to explore technical aspects further are encouraged to consult with the instructor individually. This approach reflects an instructional philosophy that prioritizes doing and observing over passive listening while maintaining inclusivity and accessibility for all students.

Taken together, the instructional strategies and learning activities in ITC 18000 are designed to support experiential learning, interdisciplinary relevance, and practical cybersecurity literacy. By

emphasizing reflection, case analysis, and real-world application, the course prepares non-technical students to engage responsibly with cybersecurity challenges without requiring advanced technical expertise.

Sample Learning Activities and Assignments

To support experiential learning and reinforce the practical application of cybersecurity concepts, ITC 18000 incorporates a range of structured activities and assignments that connect course content to students' everyday digital experiences. These activities are intentionally designed to be accessible to non-technical learners while promoting reflection, analysis, and application.

One representative activity involves analyzing phishing communications. Students are presented with sample emails or real-world phishing attempts and asked to identify indicators of fraudulent or malicious intent. They evaluate elements such as sender information, embedded links, language patterns, and contextual cues. Following this analysis, students explain their reasoning and discuss how similar attacks could impact them personally or within a professional environment. This activity emphasizes recognition of common threats while reinforcing critical evaluation skills.

Another common assignment focuses on personal cybersecurity practices, particularly password management and account security. Students are asked to reflect on their current digital habits, including password reuse, authentication methods, and personal account protection strategies. They then compare their practices to established cybersecurity recommendations and identify areas for improvement. This reflective exercise encourages students to connect course concepts to their own behavior and supports movement from awareness to informed action.

Case-based learning is also used extensively throughout the course. Students analyze real-world cybersecurity incidents, such as data breaches, ransomware attacks, or privacy violations, and evaluate the causes, consequences, and responses associated with each case. These assignments require students to locate relevant information, assess the credibility of sources, and apply course concepts to interpret complex situations. Rather than focusing on technical forensic analysis after the fact, the emphasis is placed on understanding risk, decision-making, and organizational impact.

The course culminates in an individual research project that allows students to explore a cybersecurity topic aligned with their academic or professional interests. Students conduct research, develop a written report, and present their findings, demonstrating their ability to synthesize course concepts and apply them to real-world contexts. Topics often reflect interdisciplinary connections, with students selecting issues relevant to their major or anticipated career field. This project reinforces higher-level thinking skills while maintaining the course's focus on accessibility and practical relevance.

Collectively, these activities illustrate how experiential learning principles are operationalized in the course. Students engage with familiar experiences, reflect on their assumptions and behaviors, develop conceptual understanding, and apply their knowledge to new situations. By

emphasizing relevance, reflection, and real-world application, these assignments support the development of meaningful cybersecurity literacy among non-technical learners.

Student Engagement and Interdisciplinary Relevance

Student engagement in ITC 18000 was closely tied to the course's emphasis on relevance and personal connection to cybersecurity concepts. Throughout the semester, students were encouraged to draw on their majors, career interests, and anticipated professional environments as they engaged with the course material. This approach helped position cybersecurity as a shared concern across disciplines rather than an isolated topic within computing fields. Students frequently framed discussions and assignments around how security practices might apply to their future roles, reinforcing the course's interdisciplinary intent.

Many students entered the course with a baseline familiarity with everyday security practices, such as using strong passwords, enabling multi-factor authentication, and recognizing phishing attempts. These experiences often stemmed from institutional requirements or prior exposure rather than formal instruction. The course is built on this foundational awareness by helping students move beyond compliance-based behaviors toward a deeper understanding of why such practices matter and how security failures can impact individuals and organizations. As the semester progressed, students demonstrated an increasing ability to articulate cybersecurity risks and responsibilities in more nuanced, context-specific ways.

Interdisciplinary engagement was also evident in students' selection of discussion topics and in their individual research projects. Students from more technically oriented majors tended to pursue topics that explored deeper technical or system-level issues, even though the course did not require technical implementation. In contrast, students from non-technical disciplines often selected well-known cybersecurity incidents, organizational breaches, or privacy-related topics that aligned with their academic interests. This flexibility supported meaningful engagement while reinforcing the applicability of cybersecurity concepts across fields.

Student participation improved noticeably throughout the course. Many students, particularly first-year students, began the semester as passive participants, often hesitant to contribute to discussions. Over time, as students became more comfortable with the course structure and content, engagement increased. Discussions became more active and reflective, with students drawing on personal experiences, current events, and course concepts to support their contributions. This progression suggests that the emphasis on reflection and relevance strengthened students' confidence and their willingness to engage with cybersecurity topics.

Overall, ITC 18000 fostered student engagement by emphasizing interdisciplinary relevance, personal connection, and reflective learning. By encouraging students to view cybersecurity through the lens of their own academic and professional aspirations, the course supported meaningful participation. It helped students recognize cybersecurity literacy as an essential component of informed citizenship and workforce readiness.

Course Impact and Preliminary Outcomes

While formal assessment of learning outcomes is ongoing, several preliminary observations provide insight into the impact of ITC 18000 on student engagement and cybersecurity awareness. These observations are drawn from course discussions, reflective assignments, and instructor evaluation of student work.

Students demonstrated an increased ability to recognize and articulate cybersecurity risks in both personal and professional contexts. Early in the course, many students described cybersecurity primarily in terms of basic practices such as password use or antivirus software. As the semester progressed, students began to engage more deeply with concepts such as risk, vulnerabilities, and organizational responsibility, often applying these ideas to scenarios relevant to their academic disciplines and future careers.

Student engagement also increased over time, particularly in discussion-based and reflective activities. Many students initially approached cybersecurity topics with hesitation, especially those from non-technical majors. However, as the course emphasized familiar contexts and personal relevance, participation became more active and substantive. Students increasingly contributed examples drawn from current events, personal experiences, and disciplinary perspectives, indicating greater confidence in engaging with cybersecurity concepts.

Interdisciplinary connections emerged as a consistent theme in student work. Students frequently framed cybersecurity issues in relation to their intended professions, demonstrating an ability to connect course concepts to diverse fields, including business, healthcare, education, and the social sciences. This suggests that positioning cybersecurity within a general education framework supports broader applicability and relevance.

These observations suggest that an experiential, reflection-centered approach can support the development of cybersecurity awareness among non-technical learners. At the same time, they highlight the need for more systematic assessment in future iterations of the course to better measure learning outcomes and long-term impact.

Lessons Learned and Implications for Practice

The development and delivery of ITC 18000 revealed several instructional challenges and corresponding lessons learned related to student composition, engagement, and instructional design that may be useful to educators developing cybersecurity courses for non-technical audiences.

One notable outcome was the enrollment of technically oriented students, particularly from computer science, despite the course being designed primarily for non-technical majors. Their interest highlighted the value of an introductory, conceptually focused cybersecurity course as an early point of exposure across disciplines, especially given that formal security coursework in many programs is introduced later in the curriculum.

Students demonstrated a strong interest in the relevance of cybersecurity to their future employment and professional responsibilities. Many recognized the ethical dimensions of cybersecurity and engaged deeply with discussions surrounding social media, misinformation, and the rise of deepfake technologies. These topics resonated strongly and reinforced the

importance of framing cybersecurity as a socially embedded and ethically grounded issue rather than a purely technical concern.

Reflective activities emerged as one of the most effective instructional strategies in the course. Structured reflections consistently generated the most substantive discussions, as students drew on personal experiences, disciplinary perspectives, and contemporary examples. While students did not resist technical content, the limited technical assignments included in the course revealed challenges for some learners, underscoring the importance of carefully balancing technical depth in a mixed-audience environment. Reflection-based activities enabled all students to participate meaningfully regardless of prior technical background.

Over the course of the semester, non-technical students became increasingly comfortable engaging with cybersecurity concepts and showed less intimidation than during their initial participation. This progression suggests that an experiential, reflection-centered approach can support the development of confidence and conceptual understanding among students who may initially perceive cybersecurity as inaccessible or overly technical.

Balancing technical depth across a diverse student population proved to be one of the most persistent instructional challenges. Managing a mix of online and in-person students further complicated course delivery. Future offerings may benefit from being designed explicitly for either an online or face-to-face format, allowing for more consistent pacing, interaction, and activity design. Additionally, reviewing the academic backgrounds of enrolled students earlier in the semester could support a more targeted selection of examples and scenarios aligned with students' disciplinary interests.

Several design trade-offs were made intentionally. Extensive hands-on technical assignments were avoided due to concerns about unequal access to technology and the risk of unintended system changes on students' personal devices. As a result, the course relied more heavily on freely available online tools, demonstrations, and scenario-based activities. While this approach supported accessibility and equity, it also revealed opportunities for future refinement.

From a broader instructional perspective, this course highlights several considerations for educators designing cybersecurity experiences for non-technical learners. Device variability, student anxiety related to technical content, and the importance of interdisciplinary framing all play critical roles in course design. Situating cybersecurity within general education structures can significantly expand access and participation, but doing so requires clear communication with academic advisors regarding course content, expectations, and appropriate student populations.

Looking ahead, future iterations of ITC 18000 may incorporate optional technical experimentation through controlled environments such as virtual machines or virtual desktop infrastructures. These tools would allow interested students to explore technical concepts more deeply without compromising accessibility or system integrity, preserving the course's experiential and inclusive focus while expanding opportunities for applied learning.

Conclusion

As digital technologies continue to shape personal, academic, and professional environments, cybersecurity awareness has become an essential competency across disciplines. This paper presented the design of ITC 18000 – Introduction to Computer Security, a three-credit course developed to introduce foundational cybersecurity concepts to non-technical learners through an accessible, experiential, and interdisciplinary approach. Rather than emphasizing technical implementation, the course frames cybersecurity as a set of informed practices and decisions embedded in everyday digital life.

Grounded in experiential learning, the course leverages familiar contexts, structured reflection, and case-based analysis to lower barriers to participation while maintaining conceptual rigor. This design supports confidence development among non-technical students and reinforces cybersecurity literacy as a shared responsibility rather than a specialized technical domain. Placement within general education and an interdisciplinary cybersecurity minor further broadens access and encourages students to consider the ethical, professional, and societal dimensions of cybersecurity.

The instructional strategies and design choices described in this paper offer practical guidance for educators seeking to integrate cybersecurity education beyond traditional computing programs. Key considerations include balancing accessibility with depth, accommodating diverse technical environments, and emphasizing reflection and real-world relevance. While the course intentionally limited hands-on technical implementation, future iterations may explore optional technical extensions using controlled environments, such as virtual machines, to support deeper engagement for interested students without compromising inclusivity.

Future work may also include systematic assessment of learning outcomes and a longitudinal examination of cybersecurity awareness across disciplines. Collectively, these efforts can contribute to a broader understanding of how experiential, interdisciplinary approaches can support meaningful cybersecurity literacy for non-technical learners.

References

[1] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. Gaithersburg, MD, USA: NIST, Apr. 2018.

[2] Association for Computing Machinery, *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, New York, NY, USA, 2017, doi: 10.1145/3184594.

[3] S. M. Redman, K. J. Yaxley, and K. F. Joiner, "Improving general undergraduate cyber security education: A responsibility for all universities?" *Creative Education*, vol. 11, no. 12, pp. 2541–2558, 2020, doi: 10.4236/ce.2020.1112187.

[4] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Education, 2015.

[5] Purdue University Fort Wayne, "Interdisciplinary Ways of Knowing," *Undergraduate Catalog*. Available: https://catalog.pfw.edu/content.php?catoid=66&navoid=4021

[6] Purdue University Fort Wayne, “Cyber Security Minor,” *Undergraduate Catalog*. Available: https://catalog.pfw.edu/preview_program.php?catoid=66&poid=19304&returnto=4023

[7] Y. Zhou, “Cybersecurity and Privacy Protection in the Digital Age: Challenges and Countermeasures,” pp. 1–6, Jun. 2025, doi: 10.1109/bmsb65076.2025.11165675.

[8] D. A. Kolb, Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs, NJ, USA: Prentice-Hall, 1984.x

[9] B. S. Bloom, *Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain*. New York, NY, USA: Longmans, Green, 1956.

[10] G. N. M. Dixit and K. A. Thomas, “Transformative pedagogy integrating Bloom’s taxonomy, David Kolb’s experiential learning and neuro-systemic dynamics in learning,” in Transformative Pedagogies and Digital Learning, Cham, Switzerland: Springer, 2021, pp. 3–25, doi: 10.1007/978-3-030-72400-9_1.