Design and Development of an Interactive Web-based Platform for Learning Common Cyber Threats through Quizzes

Will Agyei
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

Suhair Amer
Department of Computer Science
Southeast Missouri State University
Cape Girardeau, Missouri, USA

ABSTRACT
Users of this project can utilize a website with supporting multiple, interactive and responsive learning systems that teach them how to identify and respond to the most common types of cybercrime. The website includes 10 short, interactive lessons on identifying the following primary types of cyber threats (Malware, Phishing, Ransomware, Spyware/Adware, DDoS Attack, Man-in-the-Middle Attack, SQL Injection, Password Attack, Social Engineering, Supply Chain Attack). Each lesson has a built-in quick check question designed to reinforce what has been learned, and the quiz engine provides the user with randomly selected questions that allow them to receive immediate feedback and track their progress. The system was created using HTML, CSS, and Vanilla JavaScript to create a high level of performance, minimal load time, and compatibility across multiple types of devices. The user interface is designed to provide clear, easy to navigate, accessible and mobile-friendly interfaces. Users can store their progress locally in their browser and do not need an account or external database, therefore protecting their privacy. Overall, the work is a lightweight, user-friendly educational platform to help users develop their skills through repeated practice and retention of information.

Keywords
Cybersecurity Education, Cyber Threat Awareness, Interactive Learning, Web-Based Learning Platform, Quiz-Based Learning, Information Security Awareness, Gamification, Educational Technology, Cybersecurity Training, User Engagement.

1. INTRODUCTION
Cybersecurity threats continue to grow in both number and complexity, affecting individuals regardless of their technical experience. While organizations increasingly invest in security technologies, human error remains one of the leading causes of successful cyberattacks. Common threats such as phishing, malware, weak passwords, social engineering, and identity theft often exploit a lack of user awareness rather than technical vulnerabilities. As a result, cybersecurity education has become an essential component of digital safety.

Despite the availability of online security awareness programs, many educational resources present challenges for beginners. Training materials are frequently text-heavy, use technical terminology, or require significant time commitments, which can discourage engagement and reduce knowledge retention. Furthermore, some systems focus primarily on information delivery rather than providing opportunities for learners to actively apply and test their understanding. Effective cybersecurity education should therefore prioritize simplicity, accessibility, and user interaction while supporting long-term learning outcomes.

This paper presents the design and implementation of a browser-based cybersecurity learning platform aimed at beginners. The system introduces learners to ten fundamental categories of cyber threats through concise lessons written in clear, easy-to-understand language. Each lesson includes a short knowledge check that provides immediate feedback, allowing users to reinforce concepts as they progress through the course. To further strengthen understanding, the platform incorporates randomized quizzes that combine content from multiple lessons and deliver instant performance results.

The proposed system adopts a Single-Page Application (SPA) architecture that organizes content into four primary sections: Home, Lessons, Quizzes, and Progress Report. Lessons are displayed dynamically within a central viewing area, while navigation remains consistent across the application. Progress tracking is achieved through local browser storage, enabling users to save their achievements and monitor improvement without creating an account or transmitting personal data to external servers. This approach supports user privacy while maintaining a seamless learning experience.

Accessibility and usability are central considerations in the platform's design. The interface employs responsive layouts using modern web technologies to support desktop, tablet, and mobile devices. High-contrast color schemes, touch-friendly controls, ARIA labels, and live feedback regions help ensure that the system remains usable by a broad range of learners. The design also emphasizes readability through balanced spacing, clear typography, and minimal visual distractions. The platform was developed using HTML, CSS, and JavaScript, with a focus on maintainability and future extensibility. Particular attention was given to creating a structured content model, implementing fair quiz randomization, maintaining interface stability during question transitions, and providing concise yet informative feedback. The resulting source code is modular and well

documented, allowing future developers to extend the system or integrate its components into related educational applications.

By combining microlearning principles, interactive assessments, progress tracking, and accessible interface design, the proposed platform seeks to provide an engaging and practical introduction to cybersecurity awareness. The project demonstrates how modern web technologies can be used to create an effective educational tool that supports beginner learners in developing essential cyber threat recognition skills.

2. LITERATURE REVIEW

Cybersecurity threats continue to increase in complexity, speed, and scale as attackers adopt automation, artificial intelligence, and more psychologically sophisticated strategies. Modern attacks increasingly target human behavior rather than technical vulnerabilities, exploiting trust, urgency, and routine workplace habits. Organizations continue to invest in training, but the academic and industry evidence shows that traditional awareness programs often fail to create long-term behavioral change. This literature review synthesizes findings from threat-intelligence reports, academic studies, and human-centered cybersecurity research, highlighting the limitations of current approaches and the potential of microlearning, gamification, and HCI-aligned designs to build more effective learning tools [1].

Recent threat-intelligence reports consistently show that attackers increasingly rely on phishing, credential theft, email-borne malware, and social engineering as primary entry points to systems. IBM's X-Force Threat Intelligence Index identifies misuse of valid credentials as the leading source of initial access, reflecting a shift from technical exploitation to identity abuse [2]. DeepStrike's 2025 threat analysis similarly reports a rise in AI-generated phishing emails, more convincing spoofed login pages, and automated reconnaissance that allows attackers to customize lures to individual users [1]. Varonis' industry report adds that password reuse, unpatched systems, and human error remain leading contributors to breach severity, particularly in cloud environments [3][4].

Human vulnerability appears consistently across these sources. A global authentication survey by Yubico found that fewer than half of employees could reliably recognize AI-generated phishing emails, and many admitted opening suspicious messages due to workload pressure or assumptions of legitimacy [5]. The trend across reports suggests that the "human attack surface" is now one of the most actively exploited weak points in organizational security, reinforcing the need for training approaches that address behavior in realistic contexts [1].

Organizations have attempted to address these risks with cybersecurity awareness programs, yet academic evidence shows inconsistent outcomes. A systematic review by Prümmer and colleagues found that many training programs temporarily increase knowledge or confidence but do not consistently change long-term behavior [6]. In small and medium-sized organizations, simulated phishing campaigns and repeated workshops showed some reductions in click rates, but only when reinforcement was frequent and content was tailored to specific risks [7].

Large-scale replications grounded in the NIST Phish Scale reveal that many common training formats, especially annual or compliance-oriented sessions, fail to improve reporting behavior or reduce click rates in meaningful ways [8]. Rozema and Davis report that even trending training models show no significant change in outcomes when learners receive generic, infrequent lessons that lack real-world fidelity [9].

Across the literature, recurring weaknesses include long sessions that overwhelm learners, text-heavy modules that fail to engage, and content that does not address diverse learner profiles. Short follow-up windows and narrow participant samples further limit the reliability of results. These findings highlight the need for learning approaches that are shorter, more flexible, more contextual, and more aligned with how people naturally acquire skills [6].

Microlearning has emerged as a promising alternative because it delivers information in small, focused segments—typically three to five minutes—that learners can access at their own pace. Industry reports note that distributed, bite-sized learning aligns more closely with the way busy employees absorb information during the workday [10][11][12]. TerraNova Security emphasizes that microlearning improves retention by spacing out exposure to key concepts instead of overwhelming users with long sessions [10].

Academic evidence supports these claims. Le's doctoral project demonstrated that short videos, brief readings, and quick quizzes produce greater engagement and higher post-test scores than traditional single-session training formats [13]. Agrianidis' study on serious games and microlearning found that learners who received small, tightly focused lessons were more likely to recall information accurately weeks later. Microlearning also reduces cognitive load, making it particularly effective for non-technical users who may feel intimidated by cybersecurity terminology [14].

Gamification and serious games are increasingly used to improve motivation and engagement in cybersecurity learning. A review by Gwenhure and colleagues found that game elements—such as points, scenario challenges, and story-based decision-making—help increase participation and encourage repeated practice [15]. Pahlavanpour and Gao's mapping study shows that gamified awareness programs often outperform passive training by creating interactive, psychologically safe environments where learners can experiment without real consequences [16].

Empirical work supports these findings. Alotaibi et al. designed a mobile game for basic cybersecurity education that significantly improved awareness scores compared to written materials [17]. Hill, Fanuel, and Yuan's comparative study of security education games highlighted that visual richness, immediate feedback, and relatable scenarios are key drivers of engagement [18]. Moumouh's systematic review reinforces that interactive games encourage deeper learning but notes that many tools are evaluated only short term and often rely on technical or student-heavy samples. Across these studies, effective gamification depends on meaningful integration: game mechanics must reinforce security concepts rather than act as superficial rewards. Research consistently shows that purpose-aligned gamification offers strong potential when grounded in realistic threat scenarios and clear learning outcomes [19].

Human-Centered Cybersecurity (HCC) and Human–Computer Interaction (HCI) emphasize designing systems that support users' needs, mental models, and real-world contexts. The NIST HCC Program focuses on usability, cognitive load, and intuitive security workflows that reduce opportunities for mistakes [20]. Zimmermann and colleagues describe this shift as moving from viewing users as "weak points" to seeing them as essential partners in cybersecurity practices [21].

Albarrak's work in smart energy systems shows that confusing or overloaded interfaces increase the likelihood of insecure shortcuts, whereas clear, consistent design helps reinforce safe choices [22]. Grobler's 3U framework—user, usage, usability—argues that effective cyber defense requires understanding not just who the user is, but how they engage with systems and what barriers limit secure behavior [23]. Recent HCC studies in AI-enabled homes reveal that people respond best to interventions that provide simple explanations, match their everyday language, and allow safe experimentation. These principles directly apply to cybersecurity training. Learning tools designed with HCI principles—such as predictable navigation, clear feedback, and relatable examples—make it easier for users to understand risks, practice decisions, and retain knowledge. A positive, judgment-free learning environment also encourages users to explore unfamiliar concepts without fear of repercussions [24].

3. DESIGN

Across the literature, several consistent themes emerge indicating that effective cybersecurity education must:
• recognize users as partners.
• deliver content in small, manageable pieces.
• use meaningful gamification to maintain engagement.
• connect lessons to realistic scenarios users face daily.

Current training tools often fall short due to short-term evaluations, narrow participant samples, or failure to adapt to evolving threats such as AI-enabled phishing [24]. A browser-based interactive tool that integrates microlearning, gamification, and HCI principles is well positioned to address these limitations. By presenting realistic decision-making scenarios—such as identifying suspicious links or evaluating login prompts—learners can practice applying security habits in a safe, low-pressure environment.

For this project, a simple and straightforward language was used to explain the 10 most important types of cyber threats, providing a healthy balance of concise, easily read lesson content. Also, Incorporated immediate feedback and instant results for users who take the quizzes or do activity checks as a way to increase their learning and retention of information. An intuitive and responsive interface was created that works on all types of mobile platforms; provides flexibility with layout and high-contrast colors; offers the same navigation throughout the entire course. Learners were allowed to have the ability to locally save their progress, which allows them to know the level of improvement without requiring an account or access to server data. Finally, provided clear, modular, and well-documented source code that can be used to extend or integrate into other similar systems in the future.

3.1 Target users

The target users are beginners seeking a foundational understanding of cyber threats. They need content that is short, reliable, and easy to understand, with opportunities to practice identifying threats in a low-friction, low-pressure environment.

3.2 Requirements and System Functions

Each user is required to and can:

- Read each lesson.
- Complete the embedded quick-check question.
- Take quizzes that mix content from all lessons.
- View progress across lessons and quizzes.

System functions include:

- Render lesson content dynamically.
- Evaluate quick-check answers.
- Generate randomized quiz questions.
- Display immediate feedback and a final badge.
- Store progress using localStorage.
- Allow users to reset their stored progress.

3.3 Design idea

The website is organized using a single-page application (SPA) format with four sections that serve as main content areas:

- Home page (Overview and Setup)
- Lessons page (Content presented in scrollable format along with Quick Achievements).
- Quizzes page (Randomized Quiz Questions and Score).
- Progress Report page (A Graphical Representation of your Achievement during the Course).

On the left-hand side of the screen, lessons can be found in a list format; they will populate into the center panel of the webpage for viewing.

3.4 Website Design Considerations

The website was designed with the following considerations:

- Responsive: Through the use of CSS Flexbox and Grid, the website will remain responsive across desktop, tablet, and mobile devices.
- Simple Design: Through clean and simple Typographic Styles, "White Space" or Balanced Space, and limited-distraction items; the text content of this site is extremely easy to read.
- Accessible: All site interactive elements have ARIA Label(s) associated with them.
- High-Contrast: Color Themes have been implemented.
- Live Regions: used in dynamically changing feedback.
- Widely visible touch-friendly buttons.
- The navigation between the tabs on this website is consistent and predictable.
- It took a significant amount of planning to organize the data structure's status without the use of frameworks.
- It was necessary to implement a deterministic approach to randomize quizzes fairly.
- There was a specific requirement to avoid content shifting when transitioning from question to question.
- Quick check feedback needed to be concise but informative.

- The difficulty level of the lesson sections was reduced to avoid overwhelming the user with long text (lessons).
- The smooth transition between quiz questions was achieved by minimizing the amount of animation used to move from question to question.
- The improvement of the progress feedback was accomplished through the creation of badge(s) and summary displays.

4. IMPLEMENTATION

The cybersecurity learning platform was implemented as a browser-based Single-Page Application (SPA) using HTML, CSS, and JavaScript. Lesson content, quizzes, and user progress were managed dynamically through JavaScript, allowing users to navigate the course without reloading pages. Progress data was stored locally using the browser's local storage feature, enabling learners to save their achievements and resume their learning without requiring an account. CSS Flexbox and Grid were used to create a responsive interface that adapts to desktop, tablet, and mobile devices, while accessibility features such as ARIA labels, high-contrast colors, and live feedback regions were incorporated to improve usability for all users.

4.1 Tools

- Languages: HTML, CSS, JavaScript
- Editor: Visual Studio Code
- Optional Hosting: GitHub Pages / Netlify / Vercel
- Test Devices: Laptop (Chrome/Edge) and smartphone (Safari/Chrome)

4.2 Implementation decisions

- Outing: A simple mechanism for showing/hiding panels without using routing, i.e., using CSS class (active), keeps the application lightweight. This makes the application quick and easy to use.
- Data: Lessons are stored inside app.js in a JSON-like structure. New lessons can quickly be added or updates made.
- Checks & Quiz: The checks are performed as soon as a user presses the button. The Quiz:
- Answers can be randomized: The answers will be evaluated immediately.
- A score is assigned, and the score will be stored.
- A badge for each level will be displayed in bronze, silver, and gold.
- Progress Storage: The following are stored in the localStorage:
    - The last lesson answered correctly.
    - A history of quizzes (score + timestamp).

- Responsiveness: The application is documented for viewing on mobile. It uses a grid/flex layout for easy access to all devices with breakpoints set at a width of 820px to allow for easy use on a mobile device.

4.3 User interface design and user testing

The user can perform the following tasks:

- Open index.html in any modern browser. Check figures 1 and 2.
- Click Start Learning or the Lessons tab. Button located at the bottom of page. Check figures 1 and 2.
- Choose a lesson from the sidebar, read it, and answer the quick check [Figures 3, 4, 5].
- After going to the and clicking Start Quiz, user will choose answers; feedback appears immediately [Figure 6].
- User can check progress and after the final question, view the score and badge [Figures 7 and 8]. They can also open Progress to view completed lessons and quiz history.
- User can click Reset Progress at any time to clear your stored data [Figure 9]
- Admin can check the local Database as it will display the key [Figure 10]

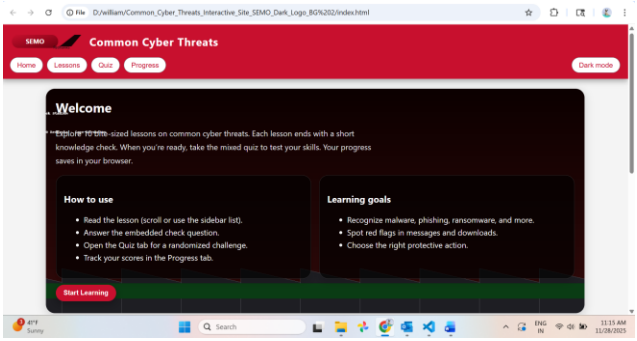

Fig 1: Home Page (light theme)

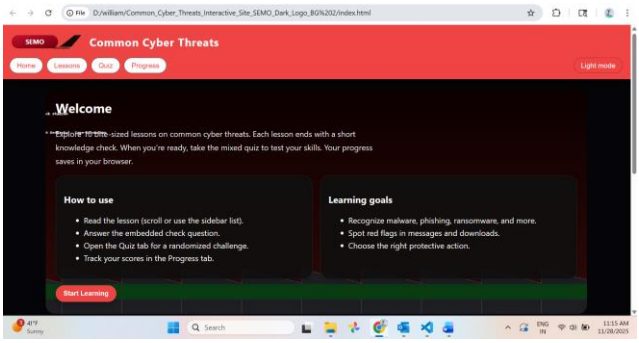

Fig 2: Home Page (Dark Theme):

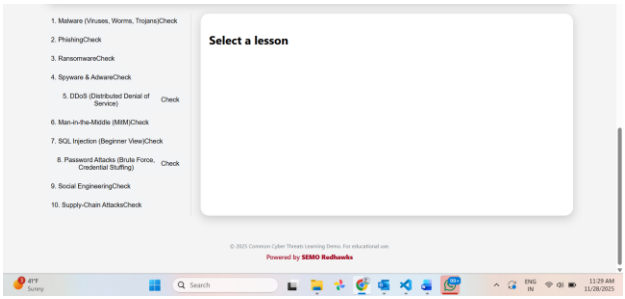

Fig 3: Lesson Before selected

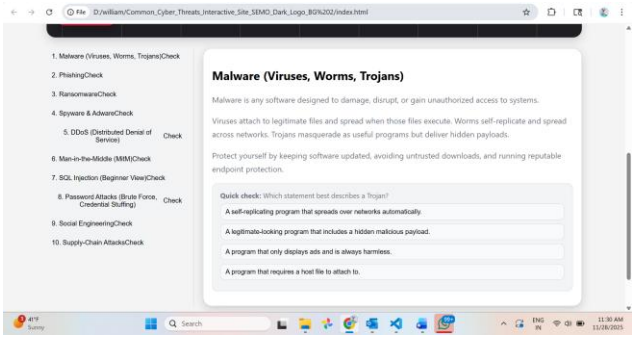

Fig 4: Lesson After selected

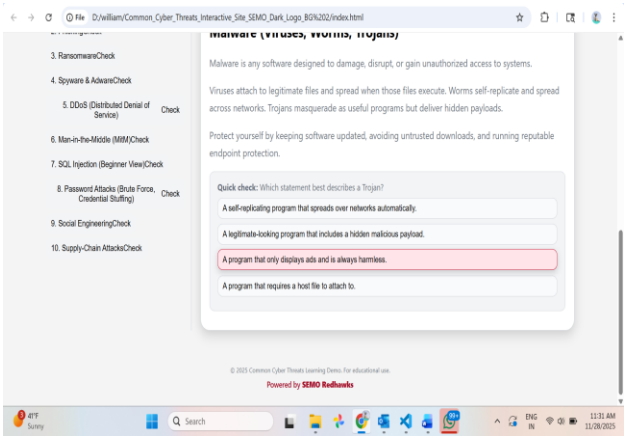

Fig 5: Option selected

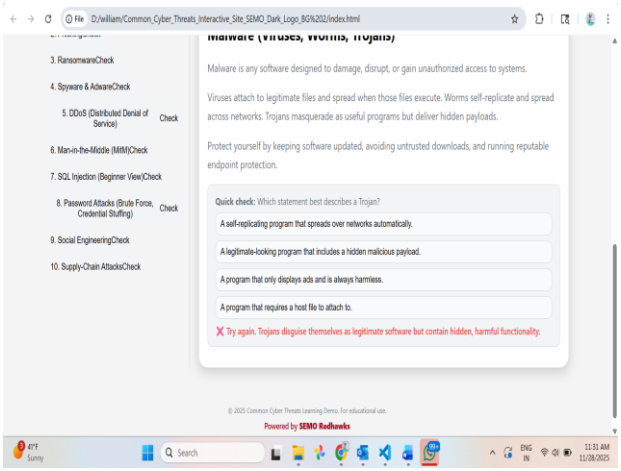

Fig 6: Feedback of option

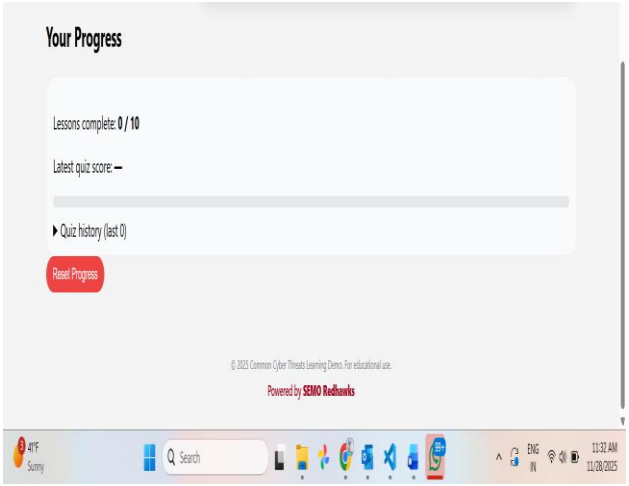

Fig 7: Progress before

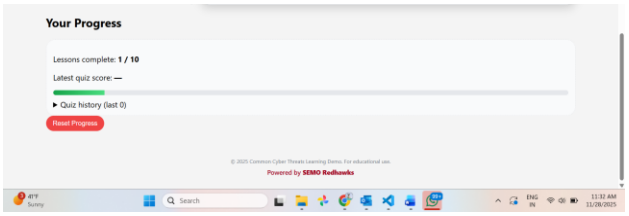

Fig 8: After quiz progress

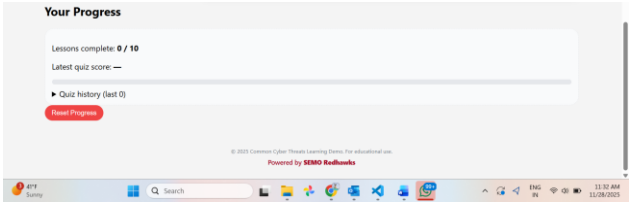

Fig 9: After clicking reset

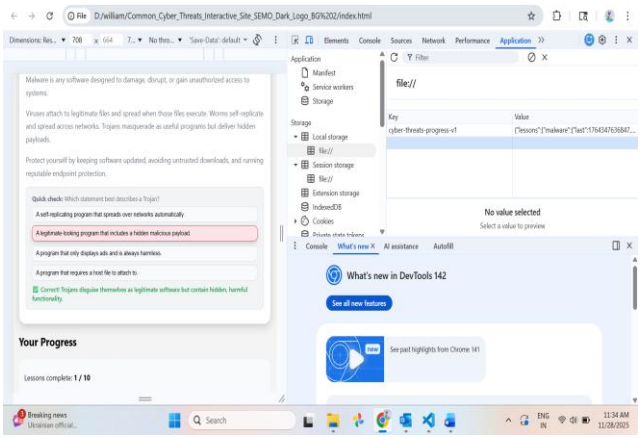

Fig 10: After quiz, the local Database will display the key (right of screen)

4.4 Practical and Ethical Considerations

The user-testing evaluation identified several practical and ethical considerations associated with the design and implementation of

the website. Because the platform is intended for a diverse user population with varying technological capabilities and usage contexts, these considerations were incorporated throughout the development process to enhance accessibility, usability, and responsible data management.

From a practical perspective, users may access the website using a range of devices, including desktop computers, tablets, and smartphones. Variations in screen size and hardware capabilities may affect the overall user experience if the interface is not fully responsive. Additionally, some users may access lessons and quizzes under conditions of limited bandwidth or unstable internet connectivity, potentially resulting in slower page loading times and reduced usability. Addressing these challenges is essential to provide equitable access to educational content regardless of device type or network conditions.

Ethical considerations were also prioritized during the development process, particularly with respect to user privacy and data protection. The website was designed to avoid collecting, storing, or transmitting personally identifiable information. Instead, only the minimum data required to support user functionality, specifically learning progress, is stored locally within the user's browser using the browser's local storage mechanism. This design reduces privacy risks, promotes transparency, and enables users to retain full control over their learning information. By limiting data collection to essential functionality, the website adheres to responsible data management practices and supports ethical standards for digital learning environments.

To address both the practical and ethical considerations identified during user testing, the website includes a "How to Access My Progress" guide located in the homepage footer. This guide explains how users can access lessons and quizzes, view how their learning progress is stored, and export their progress data when required. Additionally, a reset function allows users to delete all locally stored progress at any time. Collectively, these features enhance transparency, support user autonomy, and ensure that learners maintain control over their data while accessing the website under a variety of usage conditions.

5. RESULTS

To evaluate the effectiveness of the cybersecurity learning platform, two surveys were conducted. A quantitative survey was used to collect numerical data on user satisfaction, ease of use, content clarity, and overall learning experience through rating-scale questions. In addition, a qualitative survey was administered to gather detailed user feedback, allowing participants to describe their experiences, identify strengths and weaknesses of the system, and suggest improvements. Combining both approaches provided a broader understanding of the platform's usability, educational value, and areas for future enhancement.

The usability evaluation was conducted using a five-point Likert scale, where higher mean scores indicate stronger agreement with positive statements regarding the application's design and instructional effectiveness using the following:

- The website was easy to navigate.
- The visual design and layout were appealing
- The lessons helped me understand cyber threats effectively
- The quizzes reinforced what I learnt
- Overall, I am satisfied with my learning experience on the website.

Results demonstrated a high level of user acceptance across all evaluation dimensions, with mean ratings ranging from 4.25 to 4.75, indicating overall positive perceptions of the application. Check Figure 11. Among the evaluated dimensions, *ease of navigation* received the highest mean score (M = 4.75), suggesting that participants found the interface intuitive and easy to use. This finding highlights the effectiveness of the application's navigation structure and user-centered design, enabling users to efficiently access content and complete learning activities with minimal difficulty.

The dimensions of *visual design* (M = 4.25), *quiz effectiveness* (M = 4.25–4.50), and *overall user satisfaction* (M = 4.25–4.50) also received strong ratings, reflecting favorable user perceptions of the application's aesthetic appeal, assessment features, and overall learning experience. These results suggest that the application successfully engaged users while providing a satisfactory and supportive learning environment across multiple devices. Although all dimensions were rated positively, *lesson clarity and understanding* received the lowest mean score (M = 4.25). While this score still falls within the "Agree" to "Strongly Agree" range, it identifies an opportunity for further enhancement of the instructional content. Future revisions may focus on incorporating additional examples, demonstrations, and real-world scenarios to improve comprehension of complex cybersecurity concepts. In particular, lessons covering technical threats such as SQL Injection and Man-in-the-Middle attacks may benefit from more detailed explanations, visual illustrations, and practical examples to strengthen learner understanding and knowledge retention.

Overall, the findings indicate that users perceived the application as highly usable, visually appealing, and educationally effective. The consistently high ratings across all dimensions provide evidence of the application's effectiveness as a cybersecurity learning tool while also identifying specific areas for continuous improvement.

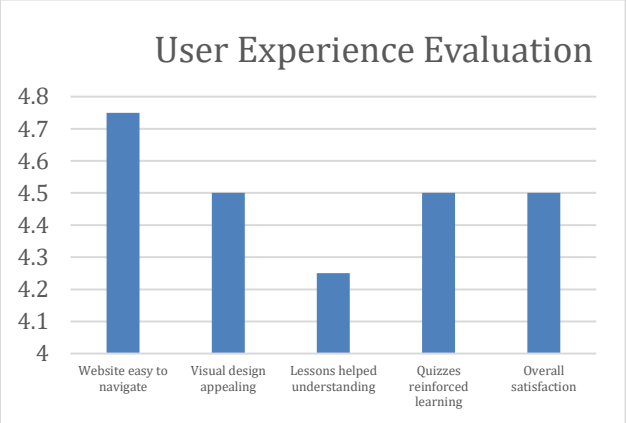

Fig 11: User Experience Evaluation results from quantitative questionnaire.

Qualitative feedback was collected through the following newly developed open-ended survey questions designed to capture

users' perceptions of the application's strengths and areas for improvement.

- What aspects of the website design did you find most effective or visually appealing?
- Which features or pages did you find confusing or difficult to navigate? Please explain.
- How clearly did the lessons explain different cyber threats? What could be improved?
- Did the embedded quizzes feel helpful for learning? Why or why not?
- Describe your overall experience using the website. What improvements would you recommend?

Thematic analysis of participant responses revealed several recurring positive themes that reflect the overall effectiveness of the application. Participants frequently highlighted the application's simple layout and visually appealing design, noting that the interface was organized, engaging, and aesthetically pleasing. Respondents also reported that the lessons were easy to understand and follow, suggesting that the instructional content was presented in a clear and accessible manner. Additionally, users described the quizzes as enjoyable, relevant, and effective in reinforcing key learning concepts, indicating that the assessment activities contributed positively to knowledge retention. Straightforward navigation was another commonly cited strength, with participants reporting minimal difficulty locating content and progressing through the learning modules.

Analysis of participant suggestions identified several opportunities for enhancement. The most frequently mentioned recommendation was the inclusion of additional icons, graphics, and visual representations within lesson content to further support engagement and comprehension. Participants also expressed a desire for more detailed explanations of complex cybersecurity concepts and threats, particularly for technical topics that may be challenging for novice learners. Furthermore, several respondents suggested incorporating additional animations and smoother transition effects between quiz questions to create a more dynamic and interactive user experience. Importantly, no significant concerns related to usability or accessibility emerged from the qualitative data. Participants generally reported positive experiences when interacting with the application, indicating that the platform effectively met user expectations regarding functionality, ease of use, and accessibility. Overall, the qualitative findings complement the quantitative results by demonstrating strong user satisfaction while identifying targeted areas for future refinement and enhancement.

6. COMMON CYBER THREATS

Table 1 summarizes the major categories of common cyber threats by outlining their descriptions, attack methods, potential consequences, and corresponding mitigation strategies. Figure 12 presents a hierarchical diagram that categorizes common cyber threats into technical, human-based, insider, and emerging threats, illustrating the relationships between each category and its associated attack types. Figure 13 illustrates a threat-to-impact flow diagram, showing how cyber threats progress from attack methods to system compromise and ultimately result in consequences such as data theft, financial loss, service disruption, and reputational damage. Table 2 presents a risk matrix that evaluates common cyber threats based on their likelihood of occurrence and potential severity, helping to identify which threats pose the greatest risk to organizations and individuals.

Table 1: common cyber threats

Cyber Threat	Description	Common Method	Potential Impact	Prevention
Phishing	Fraudulent messages that trick users into revealing information	Fake emails, texts, websites	Stolen passwords, financial loss	Verify links, use MFA
Malware	Malicious software that damages or steals data	Infected downloads, attachments	Data loss, system damage	Antivirus software, updates
Ransomware	Malware that encrypts files and demands payment	Email attachments, vulnerabilities	Loss of access to data	Backups, patch management
Password Attacks	Attempts to steal or guess passwords	Brute force, credential stuffing	Unauthorized access	Strong passwords, MFA
Social Engineering	Manipulating people into revealing information	Impersonation, scams	Data breaches	Security awareness training
DDoS Attacks	Flooding a system with traffic	Botnets	Service disruption	Traffic filtering, firewalls
Insider Threats	Threats from trusted users	Misuse of privileges	Data theft, sabotage	Access controls, monitoring

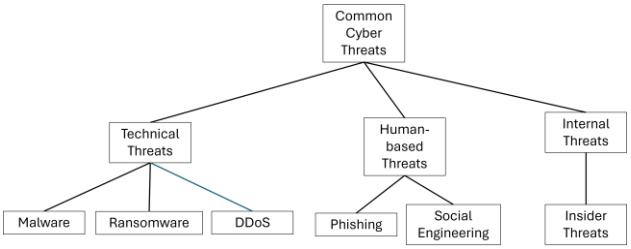

Fig 12: Hierarchical Diagram of common cyber threats

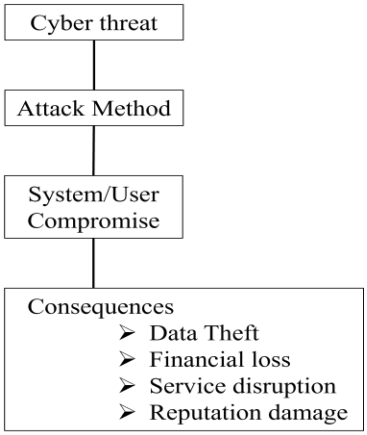

Fig 13: Threat-to-Impact Flow Diagram of common cyber threats

Table 2: Risk Matrix of common cyber threats

Threat	Likelihood	Severity
Phishing	High	High
Malware	High	Medium
Ransomware	Medium	Very High
Password Attacks	High	High
Social Engineering	High	High
DDoS	Medium	High
Insider Threats	Low-Medium	Very High

7. CONCLUSION AND FUTURE WORK

This study presented the development and evaluation of a browser-based cybersecurity learning platform designed to introduce beginners to fundamental cyber threats through interactive lessons, quizzes, and progress tracking features. The usability evaluation, conducted using a five-point Likert scale, demonstrated a consistently high level of user satisfaction across all measured dimensions. Participants reported that the system was easy to navigate, visually appealing, and effective in supporting learning, with mean scores ranging from 4.25 to 4.75. In particular, the navigation structure achieved the highest rating, highlighting the strength of the platform's intuitive and user-centered design. Quiz activities were also positively received, indicating that the system successfully reinforced key concepts and supported active learning.

Although overall results were highly positive, lesson clarity received comparatively lower scores, suggesting that some cybersecurity concepts may require further refinement to improve learner comprehension. This was supported by both quantitative and qualitative findings, which indicated a need for more detailed explanations and additional supporting visuals for complex topics such as SQL Injection and Man-in-the-Middle attacks. Nevertheless, qualitative feedback confirmed strong approval of the system's interface design, accessibility, and interactive learning approach, with users consistently describing the platform as engaging and easy to use.

Future work will focus on enhancing the instructional quality of the platform by incorporating richer multimedia elements, including diagrams, animations, and real-world case studies to improve conceptual understanding. Additional improvements may include adaptive learning pathways that adjust difficulty based on user performance, as well as expanded question banks to increase quiz variety and reduce repetition. The integration of more advanced analytics for tracking learner behavior could also provide deeper insights into user progress and engagement patterns. Furthermore, future iterations could explore optional cloud-based synchronization to allow progress tracking across multiple devices while maintaining privacy-focused design principles. Overall, these enhancements aim to further strengthen the educational effectiveness, interactivity, and scalability of the platform.

8. REFERENCES

[1] DeepStrike, "Cybersecurity Statistics 2025: Key Trends & Breach Costs," 2025.

[2] IBM Security, "X-Force Threat Intelligence Index 2025," IBM Institute for Business Value, 2025.

[3] Varonis, "139 Cybersecurity Statistics and Trends," 2025.

[4] Keepnet Labs, "Microlearning in Security Awareness Training Programs," 2025.

[5] Yubico & Talker Research, "Global State of Authentication Survey," 2025.

[6] J. Prümmer et al., "A Systematic Review of Cybersecurity Training Methods," Comput. & Security, vol. 134, 2024.

[7] H. Ascic, "Effectiveness of Cybersecurity Awareness Training for SMEs," master's Thesis, Natl. Coll. Ireland, 2023.

[8] G. Ho et al., "Understanding Phishing Training Efficacy in Practice," IEEE S&P, 2025.

[9] A. Rozema and J. Davis, "Anti-Phishing Training Inefficacy," arXiv:2506.19899, 2025.

[10] TerraNova Security, "Integrating Microlearning into Awareness Training," 2023.

[11] TrainingFolks, "Microlearning for Cybersecurity," 2017.

[12] Symbol Security, "Microlearning in Awareness Programs," 2025.

[13] D. Le, "Cybersecurity Training Using Microlearning and Gamification," Doctoral Project, 2023.

[14] A. Agrianidis, "Information Security Training and Serious Games," Master's Thesis, 2021.

[15] A. Gwenhure et al., "Gamification of Cybersecurity Awareness," Int. J. Serious Games, vol. 11, 2024.

[16] O. Pahlavanpour and X. Gao, "Mapping Study on Gamification in Security Awareness," Heliyon, vol. 10, 2024

[17] F. Alotaibi et al., "Enhancing Cybersecurity Awareness with Mobile Games," ICITST, pp. 129–134, 2018.

[18] W. Hill, M. Fanuel, and X. Yuan, "Comparing Serious Games for Cybersecurity," ASEE Conf., 2020.

[19] C. Moumouh et al., "Serious Games for Security Training," Int. J. Serious Games, vol. 12, 2025.

[20] NIST, "Human-Centered Cybersecurity Program," 2016–present.

[21] V. Zimmermann et al., "Human-Centered Cybersecurity Revisited," CACM, vol. 67, pp. 72–81, 2024.

[22] A. Albarrak et al., "Cybersecurity, Usability, and HCI in Energy Systems," Sustainability, vol. 16, 2024.

[23] M. Grobler et al., "User, Usage, Usability Framework," Frontiers Big Data, vol. 4, 2021.

[24] A. Vasalou et al., "Cybersecurity in AI-Enabled Homes," Comput. & Security, vol. 138, 2025.