Development of an Educational and Awareness Website Cybersecurity Learning System

Uriel Malavé Tripari
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project Expo, May 2026

Abstract *— Conventional cybersecurity awareness approaches usually lack sufficient interactivity and practicability, making users susceptible and prone to cyberattacks. To overcome this challenge, this project developed the Cybersecurity Learning System to meet emerging demands for cybersecurity education due to an increase in cyberattacks based on exploiting human errors, such as phishing, social engineering, malicious links, and deception. This web-based educational system was designed and implemented using technologies such as HTML, CSS, JavaScript, PHP, and MySQL. The website includes educational content modules, interactive exercises, feedback, and visual learning capabilities based on cybersecurity risks, such as phishing, malicious attachments, social network scams, pretexting, and tailgating awareness. The web system was tested to determine its capability in providing cybersecurity education, ease of use, and accessibility. It was found that the platform has effectively provided a structured and user-friendly approach to learning about cybersecurity concepts.*

Keywords *— Cybersecurity Awareness, Human Errors, Learning Capabilities, Social Engineering.*

INTRODUCTION

The emergence of digitization in current business processes has created an opportunity for cyber attackers to exploit people for their own purposes. As businesses adopt cloud computing, electronic communication, remote work, and digital means of data storage, the nature of cyberthreats continues to develop at a fast pace. Today's hackers not only base themselves on advanced technology to execute a cyberattack, but they also make great efforts to mislead people through psychological means.

Traditional cybersecurity awareness courses usually cannot cope with the advanced nature of today's cyberattacks. Many corporations still apply outdated educational solutions, like policy manuals and PowerPoint slideshows, to ensure their staff is aware of cybersecurity issues. Nevertheless, research indicates that such approaches tend to produce few positive outcomes in preparing staff members for quick decision-making in a stressful environment [1].

Moreover, most non-professional users who are not involved in the cybersecurity field lack access to simplified and structured education resources explaining what cybersecurity entails in simple terms. Explanations of cybersecurity-related issues in technical language may become discouraging enough for users seeking cybersecurity awareness, leaving them vulnerable to threats. As cyberattacks continue posing risks to individuals of varying levels of experience, there is a growing need for user-friendly educational platforms that provide users with information on cybersecurity topics.

This project addresses this gap by developing the Cybersecurity Learning System, a web-based tool that will help teach users how to gain cybersecurity awareness training via a structured learning process. Unlike lecture-style training sessions where users must listen to information, the suggested web system offers practical lessons in the form of real-life scenarios and exercises. These will include, for instance, phishing scams, malicious links/attachments, social media scams, pretexting attacks, and tailgating, thus helping to increase users' cybersecurity skills. This experiential learning approach is intended to improve knowledge retention, build user confidence, and promote safer online behavior [2].

The main objective of this initiative is to provide an educational system that helps individuals comprehend different cybersecurity risks, identify possible signs, and implement appropriate strategies for safe online behavior. With an emphasis on simplicity and ease of use, the website aims to offer cybersecurity education for beginners while trying to minimize human-related breaches.

LITERATURE REVIEW

Current literature on cybersecurity awareness highlights that human-related factors represent one of the biggest vulnerabilities for companies. Even though many corporations allocate funds into securing their infrastructure via advanced technologies, modern-day attackers try to manipulate employees using techniques such as phishing, impersonation, and other types of social engineering. For example, according to the European Union Agency for Cybersecurity (ENISA), phishing and social engineering are among the most widespread threats to an organization's security, as these attacks target human vulnerabilities rather than technical [3].

A number of articles indicate that classical methods of raising cybersecurity awareness are no longer sufficient. Thus, NCSC reports that users receive more information about cybersecurity issues when educational material is supplemented with interactive training sessions rather than when users are exposed to passively receiving such information in the form of policy papers or pre-recorded video presentations [4]. Interactive approaches to training help users practice their skills while remaining in an environment resembling reality. Additionally, cybersecurity researchers claim that many companies do not utilize the cybersecurity knowledge they already possess. As written in the article “A New Cybersecurity Research Agenda (In Three Minutes or Less),” “We would need a lot less research if we put into practice what we already know. But we don’t” [5]. This quote reveals the persistent disparity between cybersecurity information and the implementation of awareness and training programs in corporations.

Moreover, the use of phishing simulations and scenario-based exercises is proven to enhance user awareness. The Cofense study shows that companies that have been conducting regular simulations see improvements in risky user behavior and an increase in the number of reported suspicious emails [6]. This proves that through repeated exposure, users become proficient at recognizing cyberattacks.

One other subject raised by cybersecurity education research relates to accessibility and usability. Since many cybersecurity articles and guides include very technical language, they are often hard to comprehend for beginners and non-specialists. Educational scholars stress the need to employ simplified language and intuitive design to enhance educational efficiency [7]. It is particularly necessary now as cyberattacks have started targeting average internet users who do not necessarily have technical knowledge.

Furthermore, various researchers highlight the role of reinforcement and continuous learning in cybersecurity awareness applications. Studies conducted within the field of educational psychology indicate that people learn better when the learning process consists of repetitions, feedback, and interaction rather than passive activities like reading and viewing [8]. Feedback delivered promptly following exercises or simulated situations will aid in the learning process, allowing users to learn from their mistakes.

Though numerous cybersecurity awareness applications are available on the market, they are often too expensive or cater exclusively to companies rather than smaller firms and institutions. Moreover, beginners might lack the opportunity to undergo affordable and user-friendly cybersecurity training. Existing applications also concentrate heavily on phishing, paying little attention to other types of cyberthreats, including malicious attachments, social media fraud, pretexting, and tailgating. Therefore, there is still a

need for an accessible, versatile, and educational platform that could offer cybersecurity awareness training for various cyberthreats.

This literature supports the need for developing the Cybersecurity Learning System since it has established the need for using engaging cybersecurity awareness solutions that rely on real-life scenarios, simplicity, and continuous learning. The use of structured learning and hands-on training can help in enhancing cybersecurity awareness and human-related risks within the field.

METHODOLOGY

The website was created in order to provide the end-users with cybersecurity awareness training and education through well-organized training modules and interactive exercises. As previously mentioned, this platform is intended for beginners who would have an opportunity to learn about cyberattacks and cybersecurity in general thanks to the simplified educational materials. This section will present the methodology that has been used during the development of this project. The methodology will be divided into six major aspects that will be explained in detail: design, development, testing, deployment, content, and database.

Design

The website design meets the objective of creating a webpage for learning purposes based on the topic of cybersecurity. In this phase, the emphasis was placed on the creation and design of an efficient structure of a website that can be navigated easily by the users, allowing access to educational material, cybersecurity tools, and interactive tests. The website contains a navigation bar at the top, which is divided in five sections: Home, About, Content, Resources, Contact, plus the logo. When each section is clicked, it redirects the user to a different page focused on the topic indicated, changing the browser's URL accordingly. The website also contains a footer at the bottom with different hyperlinks highlighting specific system content. Depending on the section, each will provide valuable information, resources such as documents or articles, interactive exercises or a way to subscribe to the website to gain access to future content. Some have buttons or hyperlinks with different functionality that allow the user to navigate throughout the website, and these will be shown in the following sections of the report. Figure 1 illustrates the diagram of the website design. In this figure, there is a visual representation of how the website design is organized: consisting of a horizontal navigation bar, followed by the header with its content information in the middle and the footer at the bottom; each section displays its proper content.

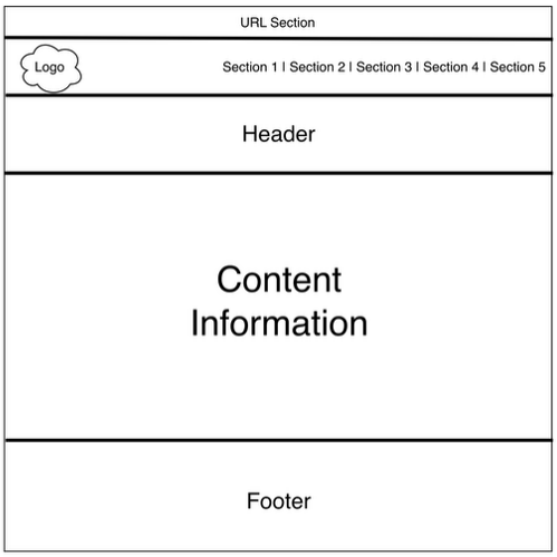

Figure 1
Website Design

Development

The website was developed during this phase through a full integration of the front end, back end, and database to form a fully functional web application. Each section integrated lessons on phishing, malicious links, social media scams, pretexting attacks, and tailgating. The content provided comprehensive explanations, warnings, preventive measures, and both theoretical and practical tests. HTML, CSS, and JavaScript were utilized for the development of the user interface, PHP was used for the management of the back-end

operations, and MySQL database was used to manage all data. Other additional functionalities, including video explanations, resources related to each topic, interactive exercises modeling a quiz, and registration forms, were added to complete the web-based application.

Testing

Testing the system involved assessing the functional capabilities, usability, and reliability of the website. Functional testing was carried out to ensure that all functionalities, such as pages, contents, quizzes, forms, and navigation tools, were working properly and without errors. Usability tests were also conducted to determine whether the system was functional and user-friendly for all kinds of users. Furthermore, tests were conducted for security and to ensure that user information was being saved accurately in the server and database.

Deployment

For the deployment stage, all coding files, documents, images, and videos were uploaded to the Hostinger web hosting server, where the website was launched and became available for use. The system was evaluated using different web browsers and devices in order to test its functionality, compatibility across different devices, and performance. After deployment, users had access to the educational materials and exercises directly from the website.

Content

The information and content on the website were dedicated solely to cybersecurity awareness and training. The information within the website was researched, structured, and presented in a simplified manner for ease of understanding by new learners. The website covered several topics, including phishing awareness, malicious links and attachment scams, social media scams, pretexting attacks, and tailgating awareness. Every topic section included information about the type of threat, common red flags, how to prevent the threat, and recommended actions to take if the threat occurred. In addition to the informational content, theoretical and practical multiple-choice quizzes were included to test the comprehension of the learner regarding the content covered in each training topic. The website also incorporated additional educational materials, including articles, documentation, and videos related to each topic, to further expand users' cybersecurity awareness knowledge. Other than the content provided, the website contained several informational sections, including the "Home" and "About" pages, which explained the website's objectives and purposes. Table 1 contains two columns showing the sections and titles of the content selected.

Table 1
Section Table

Section Number	Content Title
Section 1	Home
Section 2	About
Section 3	Content
Section 4	Resources
Section 5	Contact

Database

The project design includes mostly static front-end design, but a database has also been integrated. The role played by the database was to manage the data for those users who would like to subscribe to the website. Once the user fills out the subscription form, entering their name, email address, and message, the information is stored in the database. The database was integrated because more content will be uploaded on the website in the future, and when new content is uploaded, users can be contacted. MySQL was used to implement the database because it is compatible with the PHP language for easier integration. Table 2 represents the only table in the database, which contains the title and attributes, along with the data types that are used to store information about the subscribers.

Table 2
Database Table

Users	
Attribute	**Data Type**
id	INT
name	VARCHAR (150)
email	VARCHAR (150)
message	VARCHAR (1000)

RESULTS

This part of the project will provide, in detail, the results after the development phase was completed and its relationship with the concept proposed in the initial idea. Below, the different aspects of the website are presented.

Home Section

This section represents the homepage where users arrive when they first access the website. The homepage contains the website title and description with a brief paragraph of what the website is about. Under the paragraph, there are two buttons: the "Learn More" button, which redirects the user to the "About" page, and the "Visit Content" button, which redirects the user to the "Content" page.

The second subsection shows the objectives of the website. Each objective has a small description highlighting the purposes of the website and how it will help users improve their knowledge in the cybersecurity field. The website emphasizes three objectives:

- **Educate on Common Cyberthreats:** Explanation of key threats such as phishing, social media scams, and others.
- **Safe Security Practices:** Practical tips and best practices.
- **Support Continuous Learning:** Ongoing resource for both new and returning users.

As illustrated in Figure 2, the third subsection provides the popular training topics that will be shown throughout the website's sections. Each topic contains the title, rank, and date of the latest update. When clicking and selecting one of the topics, it will redirect the user to the "Resources" page, which provides articles or documents related to the topic selected.

Figure 2
Popular Trainings Section

The fourth subsection illustrates the "Register Now" section. This interface interacts with users who wish to subscribe to the website through a subscription form. The details requested from the users are name, email address, and phone number. All fields are required and have their own validation logic to ensure proper input data from users. After all requested fields are filled, users can click submit to send the request to the website.

The final subsection of this page is the "Footer." It is divided into 4 columns: About, Training Topics, Resources, and Support; each with its own set of hyperlinks related to the heading above. Each hyperlink redirects users to its proper content. The About column is related to what the website is about. The Training Topics takes users to a content page related to the topic selected. The Resources column links users to articles and documents related to cybersecurity. Lastly, the Support column will take users to the "Contact" page, where they can find customer support details or fill out a form for further assistance (see Figure 3).

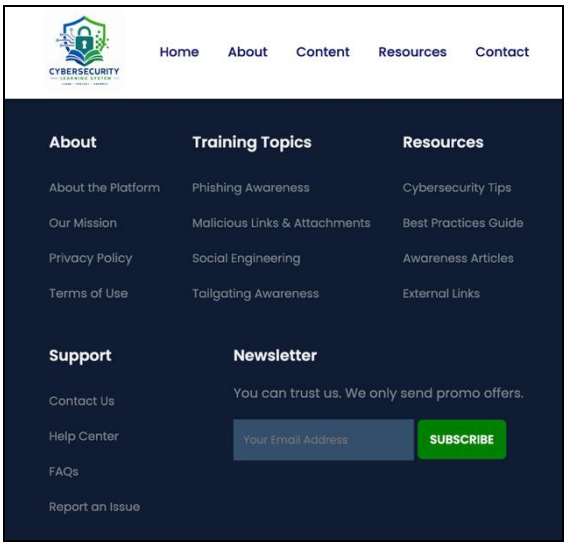

Figure 3
Website Footer

About Section

This section provides information on what the website is about, including the Vision and Mission with their fundamental purposes, and shows some of the features that are available for the users to navigate. It contains a welcoming subsection with a paragraph greeting the users to the website, and two icons below it highlighting that there are 5 cybersecurity training topics to explore, and that it is free for everyone to use.

The second subsection shows the website's features. Each feature includes a brief description highlighting available content to make users' experience in learning cybersecurity simple and engaging. The website emphasizes three features:

- **Learning Content:** Provides structured material for the users to read.
- **Documentation:** Detailed articles providing in-depth information and best practices.
- **Videos:** Media content visually explaining different topics and scenarios.

The third subsection illustrates the website's Mission and Vision. It establishes the importance of the website's goals and values and what it aims to achieve with users. Further down this subsection, there is a trusted sources section that highlights the leading academic institutions and industry leaders that approve the website's content (see Figure 4).

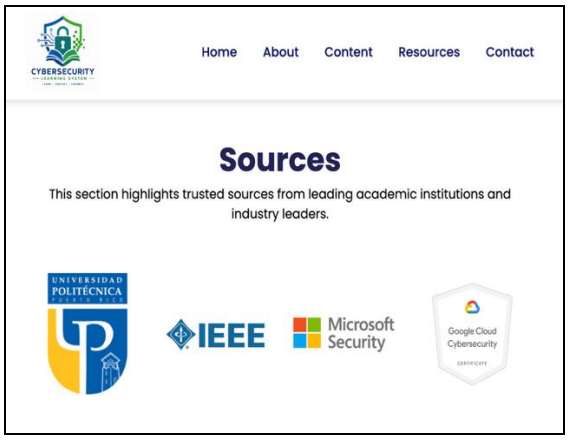

Figure 4
Sources Section

Content Section

This section provides the main content on cybersecurity threats defined throughout the website. This page will include video explanations, readable information, and a quiz section to test users' knowledge through interactive exercises and realistic scenarios. As illustrated in Figure 5, it contains a topic section where users can select which of the cybersecurity threats they would like to learn about. After clicking one of the hyperlinks or the "Read More" button, the user will be redirected to the "Content" page related to the topic selected. The following cyberthreats will be discussed in this section and throughout the website:

- Phishing Scams
- Malicious Links & Attachments
- Social Media Scams
- Pretexting Attacks
- Tailgating Awareness

The second subsection shows the "Content" page for the topic selected. When navigating to a content page, users are shown a video that explains the cybersecurity threat in detail, along with different scenarios. The video has buttons that users can control, such as play, pause, volume, full screen, and settings. Under the video, there is readable content for the users to expand on the knowledge already provided. This content describes what each cybersecurity threat is; how to identify

them; how to respond to each threat when common signs appear; and how to prevent or avoid them. All topics present different scenarios that users can either relate to or learn about. Under the readable content, there are two buttons: the "Next Topic" button and the "Test Your Knowledge" button. The "Next Topic" button redirects users to the next content page for the following topic. The "Test Your Knowledge" button leads to the quiz section, where users can test their knowledge of the information learned from the video and readable content.

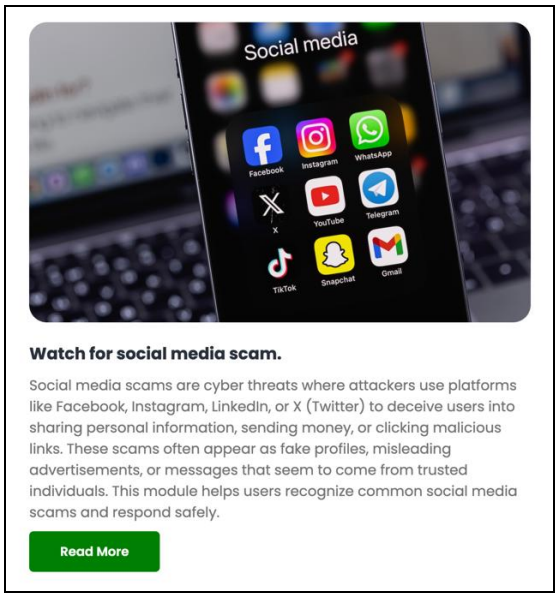

Figure 5
Content Section – Social Media Scams

The third subsection shows the "Quiz" page, which users can access by clicking on the "Test Your Knowledge" button. Each quiz consists of 5 multiple-choice questions; 3 are practical questions, for which users must select the correct answer based on different real-life scenarios; and 2 are theoretical questions to test users' knowledge of the cybersecurity threat. Each quiz window displays the title above, indicating the topic selected. Next, it shows the question in green, followed by 4 multiple-choice answers. Each quiz has its own validation logic (see Figure 6).

When the correct answer is selected, the textbox containing the answer turns green, validating that the answer selected is correct. When the wrong answer is selected, the textbox containing the wrong answer turns red, confirming that the answer selected is wrong. The moment a wrong answer is selected, the correct answer will be displayed in green, showing the correct answer to the user. After selecting an answer, an explanation appears at the bottom of the quiz window with brief feedback explaining why that was the correct or wrong answer. Also, after selecting an answer, a "Next" button appears; clicking it takes the user to the next question. When all 5 questions are answered, a test score is prompted at the end, showing the score obtained on the quiz. After finishing the quiz, the "Try Again" button appears. When the "Try Again" button is clicked, the quiz restarts, and users can redo the questions.

Figure 6
Quiz Section - Phishing

Resources Section

This section provides all resource materials on the different cybersecurity threat topics defined throughout the website. From training documents to research articles, users will get to reinforce the knowledge studied in the "Content" page by diving into additional resource materials by other researchers. This section was designed to help users select the resource material to read about according to the chosen topic. Each topic contains the title, rank, and the date the resource material was last updated. Clicking and selecting one of the topics

redirects users to a subsection of the "Resources" page that contains articles or documents related to the selected topic.

The second subsection provides a preview of the resource materials available. The preview shows an image related to the selected topic, the document title, a brief paragraph defining the topic, the author, where it was published, and the document type. This will help users get an idea of the content before clicking the "Download PDF" button. Figure 7 illustrates the "Resources" section for the Pretexting topic.

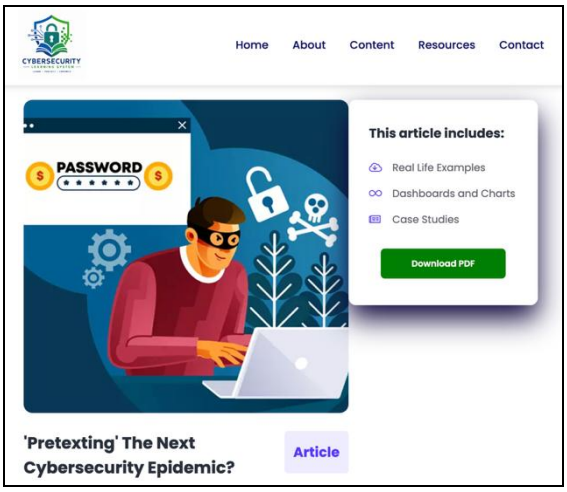

Figure 7
Resources Section – Pretexting

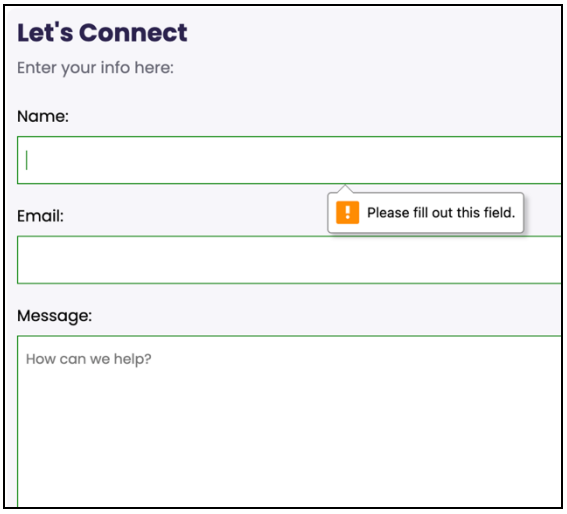

Figure 8
Contact Form

Contact Section

This section provides a form for users who want to contact the website for assistance. Users will be able to get customer support details or fill out a form to request assistance. The following details are requested from the user: name, email address, and message. These details will allow the website representative to know who they are talking to, where to reach out, and what is being requested. As illustrated in Figure 8, the contact form contains its own validation logic, suggesting that users fill out required fields before submitting the request.

DISCUSSION

The introduction of the Cybersecurity Learning System has led to the emergence of an educational website aimed at enhancing cybersecurity awareness and offering useful knowledge concerning different types of cyberthreats and their prevention. Therefore, the website includes educational material organized into cybersecurity awareness topics, including phishing, malicious links/attachments, social media scams, pretexting attacks, and tailgating awareness. As a result, users who want to learn more about cybersecurity can gain useful knowledge through a user-friendly and accessible educational website that offers simple and comprehensive information on the chosen topic.

In general, all aspects of the system's performance and structure have been considered, thus ensuring convenient use and efficient navigation across the website. It is worth noting that the site's interface has been designed to ensure ease of use for both beginning and advanced users. Thus, organized navigation menus and distinct sections have ensured effective searching for specific modules, interactive exercises through quizzes, and other information provided. Moreover, colors and layouts were chosen for convenience and to provide a professional, distraction-free look for the website.

A major achievement was the successful implementation of the website's purpose related to the development of cybersecurity awareness in the simplest way possible. All the content provided detailed information on the subject and allowed learners to become aware of the most common dangers of online activities and the appropriate actions in order to minimize risks. The system provided learners with knowledge on cybersecurity warning signs, ways to avoid risks, and the proper actions required in case of suspicious activity. Additionally, there were quizzes and exercises aimed at consolidating the material learned by users. It is worth noting that this project allowed the implementation of user-friendly tools for visual learning, receiving explanations, and reviewing results. This was particularly important since, unlike traditional cybersecurity awareness programs, the website offered an interactive approach that helped in acquiring knowledge and skills in a fun and effective manner.

FUTURE WORK

The launch of the Cybersecurity Learning System not only met the goals of this project but also opened new development possibilities. First, it is necessary to mention that one of the major improvements that might take place in the future would include additional content on important aspects of cybersecurity, such as ransomware, secure passwords, multi-factor authentication, identity theft, cloud security, mobile device security, and secure browsing. With this expansion of the website's education component, users will be able to better understand cybersecurity risks and how to protect themselves from harm.

Secondly, another improvement that can be implemented concerns the inclusion of a special news and events page where people can learn about cybersecurity conferences, training workshops, certification events, webinars, etc. Moreover, registered users can get an automatic notification by email when new material becomes available on the website or when cybersecurity events are scheduled.

The website may further enhance interaction by including a section on cybersecurity news or blogs, where users can stay up to date with the latest cyberattacks and other cybersecurity trends and issues. The addition of a discussion and comments section on the website will give users a chance to share their views and interact with those who are interested in cybersecurity awareness. Moreover, the inclusion of a section where users can ask questions and answer questions raised by other users will contribute to the project's success and improve its collaborative nature. These suggested improvements will continue enhancing the utility of the website as an important tool for cybersecurity awareness.

CONCLUSIONS

The primary purpose of implementing the Cybersecurity Learning System project was to aid cybersecurity awareness education by offering users an easy-to-use online educational portal aimed at addressing the most commonly observed types of cyber risks and ways to use the internet safely. To achieve the goal mentioned above, it was imperative to conduct research on the growing need for cybersecurity awareness and analyze the role of educational platforms in eliminating human-caused cybersecurity risks. The website was not designed as a source of information copied from other sources, but rather as a properly structured educational portal featuring well-researched content presented to users in a simple way.

To develop educational content aimed at teaching users about different types of cybersecurity threats, it was essential to conduct a thorough investigation of existing cybersecurity topics covered in various studies, educational websites, reports, publications, articles, etc. As a result of the conducted research, five topics were selected for this website: phishing, malicious links and attachments, social media scams, pretexting attacks, and tailgating awareness. The educational

modules feature easy-to-understand explanations, warning signs, prevention methods, and ways of reacting to suspicious situations.

Ease of use, organization, and accessibility have been considered essential criteria during the development process. The website's architecture, navigation menus, and overall layout were implemented in the design process to enable users to browse the educational content, perform different tasks, and test their knowledge without difficulties. In addition, educational materials, such as articles, documentation, videos, and quizzes with interactive exercises, have been provided for users to enhance their educational process and provide additional information on cybersecurity awareness.

Generally, it can be said that the project met the main objectives by building an effective and engaging cybersecurity awareness website, which is a learning tool combining education materials, interactive exercises, reliable resources, and a user-friendly interface within one place. The Cybersecurity Learning System shows how web learning platforms may be useful for building cybersecurity awareness, along with acquiring the basic knowledge and skills needed to stay safe on the internet. As cyberthreats continue to develop, educational platforms like this one will play an important role in helping people identify threats, behave safely online, and reduce human-related cybersecurity incidents.

REFERENCES

[1] NIST. (2017, June 17). *Cybersecurity Awareness, Education, and Workforce Development* [Online]. Available: https://www.nist.gov/cybersecurity-awareness-education-and-workforce-development.

[2] L. Spitzner and D. DeBeaubien, *SANS 2022 Security Awareness Report*, SANS Institute, Bethesda, Maryland, USA, 2022.

[3] ENISA. (2023, Oct. 19). *ENISA Threat Landscape 2023: July 2022 to June 2023* [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[4] NCSC. (2021, December 21). *Top tips for staying secure online* [Online]. Available: https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online

[5] D. Geer. (2011, November 11). *A New Cybersecurity Research Agenda (In Three Minutes or Less)* [Online]. Available: https://threatpost.com/new-cybersecurity-research-agenda-three-minutes-or-less-110711/75854/.

[6] Cofense. (2019). *Cofense Annual Phishing Report 2019* [Online]. Available: https://cdn.comparitech.com/wp-content/uploads/2025/02/cofense-phishing-report-2019.pdf.

[7] G. R. Morrison, et al., *Designing Effective Instruction*, 8th ed. Hoboken, NJ: Wiley, 2019.

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