



Development of an Educational and Awareness Website Cybersecurity Learning System

Uriel Malavé Tripari

Advisor: Alfredo Cruz, Ph.D.

Master in Computer Science

Graduate Project EXPO, May 2026

Abstract

Conventional cybersecurity awareness approaches usually lack sufficient interactivity and practicability, making users susceptible and prone to cyber-attacks. To overcome this challenge, this project developed the Cybersecurity Learning System to meet the emerging demands for cybersecurity education among people due to an increase in the use of cyber-attacks 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, scams on social networks, 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 out that the platform has effectively provided a structured and user-friendly approach to learning about cybersecurity concepts.

Introduction

The emergence of digitization in current business processes has created an opportunity for cyber attackers to use people for their own purposes. Today's hackers not only base themselves on advanced technology to execute a cyber-attack; instead, they make a great effort in misleading people through psychological means. Traditional cybersecurity awareness courses usually cannot cope with the advanced nature of today's attacks.

Background

- The most prevalent cyber-attacks by hackers are due to reliance on trust, manipulation and user psychology. [1]
- Users lack the skills acquired during a practical experience, causing human-based cyber incidents. [2]
- Experiential learning approach is intended to improve knowledge retention, confidence and online behavior. [3]
- Educational scholars stress the need to employ simplified language and intuitive design to enhance educational efficiency. [4]

Problem

Key issues with cybersecurity within users currently lies in inadequate cybersecurity awareness training. Due to such difficulties, there is a great need for an intuitive and easy-to-use platform for raising cybersecurity awareness, which would provide clear information and practical lessons related to various cyber-attacks. The lack of engaging platforms is among the factors that result in human-based cybersecurity incidents.

Methodology

This project was divided in the following aspects: design, development, testing and deployment. The website design was created with an efficient structure that can be navigated easily by users, allowing access to educational material, cybersecurity tools and interactive tests.

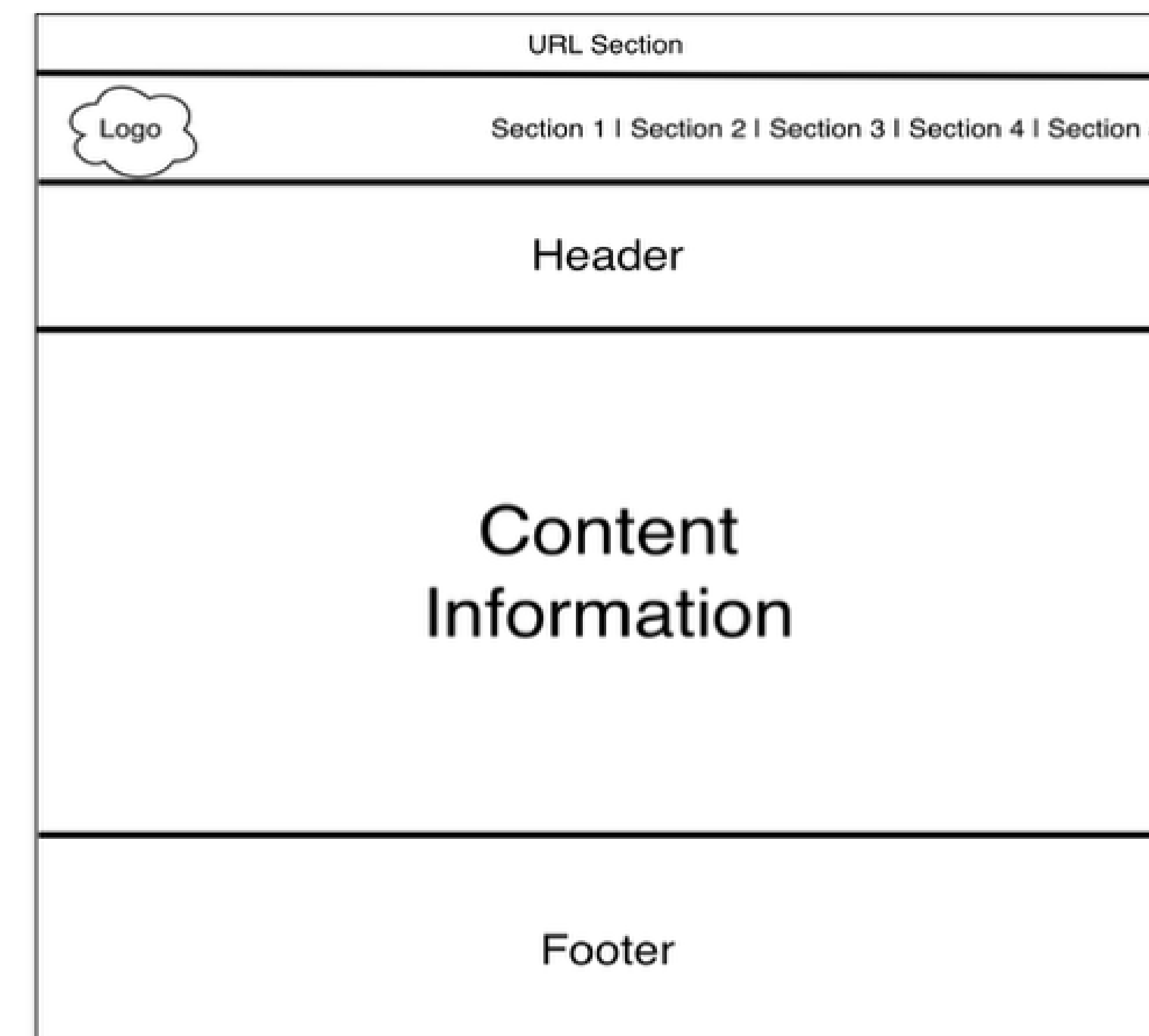


Figure 1. Website Design for the Cybersecurity Learning System

As shown in Table 1, the website's content was categorized in five primary sections, ensuring convenient use and efficient navigation throughout the platform.

Table 1. Section Table

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

The design for the project includes a database integration. The role played by the database is to manage the data for those users that would like to subscribe to the website.

Table 2. Database Table

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

Results and Discussion

The website was developed to provide user-friendly cybersecurity awareness education through organized modules and interactive content. Figure 2 depicts the content section for social media scam where users learn to identify suspicious online behavior, misleading messages and impersonation attempts commonly found.



Watch for social media scam.

Social media scams are cyber threats where attackers use platforms like Facebook, Instagram, LinkedIn, or X (Twitter) to deceive users into sharing personal information, sending money, or clicking malicious links. These scams often appear as fake profiles, misleading advertisements, or messages that seem to come from trusted individuals. This module helps users recognize common social media scams and respond safely.

Read More

Figure 2. Content Section – Social Media Scams

Figure 3 presents an example of the Phishing quiz section integrated into the website. Users answer cybersecurity awareness questions and receive immediate feedback explaining the selected answer. This interactive approach reinforces learning, improves user engagement, and helps users better recognize common tactics and online activity.

1. Which of the following best describes a phishing attack?

A) A method used to improve internet speed.

B) A cyberattack that tricks users into revealing sensitive information.

C) A software update sent by trusted companies.

D) A way to back up personal files online.

Explanation: Phishing attacks use deception to steal passwords, financial data, or personal information.

Figure 3. Quiz Section – Phishing

Overall, the website successfully combined educational content and interactive exercises to create an accessible resource that promotes safer online practices and improves users understanding of common cyber threats.

Conclusions

The primary purpose of implementing the Cybersecurity Learning System website 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 of using the internet safely.

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 educational materials, interactive exercises, reliable resources, and 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. With the ongoing development of cyber threats, educational platforms like this one will play an important role to help people identify threats, behave safely online and reduced human-related cybersecurity incidents.

Future Work

Major improvements that might take place in the future would include the addition of more content on such important aspects of cybersecurity, such as ransomware, secure passwords, multi-factor authentication, identity theft, cloud security, and secure browsing. With such expansion on the education part of the website, users will be able to have a better idea about cybersecurity risks and how to protect themselves from any harm.

Another improvement that can be implemented concerns the inclusion of a special news and events page where users can learn about cybersecurity conferences, training workshops, certification events, webinars, among others.

References

- [1] Proofpoint, "2020 State of the Phish - Cyber Security Insights Report | Proofpoint US," Proofpoint, Oct. 22, 2018. Available: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
- [2] NIST. (2017, June, 17). *Cybersecurity Awareness, Education, and Workforce Development* [Online]. Available: <https://www.nist.gov/cybersecurity-awareness-education-and-workforce-development>
- [3] L. Spitzner and D. DeBeaubien, "SANS 2022 Security Awareness Report," SANS Institute, Bethesda, Maryland, USA, 2022.
- [4] G. R. Morrison, et al., *Designing Effective Instruction*. 8th ed. Hoboken, NJ: Wiley, 2019.