Elderly Population Cybersecurity Awareness Web Application

Kamy Bubick
U.A. Whitaker College of Engineering
Florida Gulf Coast University
Fort Myers Florida
bkbubick1396@eagle.fgcu.edu

Taylor Fisher
U.A. Whitaker College of Engineering
Florida Gulf Coast University
Fort Myers Florida
tlfisher0224@eagle.fgcu.edu

Yanisley Mendiola
U.A. Whitaker College of Engineering
Florida Gulf Coast University
Fort Myers Florida
email address or ORCID

Tova Quinones
U.A. Whitaker College of Engineering
Florida Gulf Coast University
Fort Myers Florida
tdquinones6135@eagle.fgcu.edu

Isabel Ramirez
U.A. Whitaker College of Engineering
Florida Gulf Coast University
Fort Myers Florida
iramirez8643@eagle.fgcu.edu

***Abstract*—This report includes the project overview, the process, and the results of our Team project in our Computer Security Class intended for the Elderly Population.**

I. Introduction

The Elderly Population Cybersecurity Awareness project is an educational initiative designed to improve cybersecurity awareness among the elderly. Developed by a team of students: Tova Quinones, Taylor Fisher, Isabel Ramirez, Yanisley Mendiola, and Kamy Bubick, as part of our CEN 3078 course, the project delivers an accessible and user-friendly web application aimed at a population segment particularly vulnerable to online threats. The initiative focuses on educating users through interactive modules and quizzes, providing information on cyber threats such as phishing, viruses, and malware in a format suited to the needs and capabilities of elderly users.

II. Requirements

A. goals

The primary goal of the project was to build a cross-platform assessment website that simplifies cybersecurity concepts while maintaining accessibility and usability. This includes implementing features like large fonts, minimalistic layouts, and a limited number of options per screen, which help reduce cognitive load. The content is designed to be both informative and practical, covering critical topics such as phishing (email fraud), smishing (SMS scams), and vishing (voice-based scams), as well as broader topics like adware, trojans, and computer viruses. The website also supports a bilingual interface, offering both English and Spanish to accommodate a wider audience.

III. Implementation

A. Tools Used

The development of the tool relied on a combination of web technologies including HTML, CSS, and JavaScript, all managed and version-controlled via GitHub. The final product was hosted on GitHub Pages, making it freely accessible online. The developers also used Visual Studio Code (VS Code) as their integrated development environment.

B. Features

One of the standout features of the project is its modular design, which includes a responsive sidebar navigation system and embedded quizzes that guide users through educational content. A language switcher was implemented to allow seamless toggling between English and Spanish, ensuring inclusivity for non-English speakers.

C. Planning Process

Throughout the development process, a strong emphasis was placed on user interface (UI) and user experience (UX) research. Recognizing the challenges faced by elderly users—such as visual impairment, limited mobility, and unfamiliarity with digital platforms—the team prioritized high-contrast color schemes, large buttons, and an intuitive layout. The site design was influenced by established educational platforms like Podia and Quizard, incorporating elements that balance clarity with engagement. Wireframes and UI prototypes were developed to maintain visual consistency across pages, ensuring that each page followed the same aesthetic and accessibility standards.

D. Security

From a technical standpoint, the team implemented several security features to safeguard user interactions. This includes using a Content-Security-Policy (CSP) through a meta tag to mitigate the risk of cross-site scripting (XSS) attacks and enforcing HTTPS connections via GitHub. In terms of testing, the team adopted a comprehensive strategy that included black-box testing, white-box testing, and user acceptance testing (UAT). Security testing was supported by OWASP ZAP,

a penetration testing tool, ensuring that the site was not only functional but also secure.

E. Feature Implementation

Educational content is structured across five modules, three of which were fully completed by the project's midpoint: Virus, Adware, and Trojan. Each module includes a readable article explaining the nature of the threat and a set of embedded questions that users must answer before proceeding. At the end of each module, users are presented with a final quiz to evaluate their understanding. If a user selects an incorrect answer, the system provides an explanation and recommends relevant content for review, promoting self-directed learning.

IV. Challenges

While the team encountered several challenges, including implementing quiz functionality within modular content and ensuring mobile responsiveness, these were overcome through collaborative problem-solving and iterative design improvements.

V. Future Improvements

Future enhancements proposed by the team include incorporating video modules to supplement text-based content, adding pop-up definitions for complex vocabulary, and designing visual-based quizzes that could help users better recognize threats in real-life scenarios.

VI. Conclusion

In conclusion, the Assessment Tools Elderly Population Cybersecurity Awareness project effectively meets its educational and technical objectives. It demonstrates a thoughtful approach to accessibility and cybersecurity education, offering a platform that is both informative and engaging for elderly users. The final product not only showcases the team's growing proficiency in web development and UX design but also has the potential to make a meaningful impact in improving digital literacy and safety among older adults.

References

[1] F. Cohen, "Computer viruses - Theory and experiments," Computers & Security, vol. 6, no. 1, pp. 22–35, 1987.

[2] Europol, "Ransomware: No More Ransom," Europol, 2021. [Online]. Available: https://www.europol.europa.eu

[3] Symantec, "What is Adware? How It Works & How to Remove It," Broadcom, 2021. [Online]. Available: https://www.broadcom.com

[4] McAfee, "How to Protect Against Adware and Unwanted Software," McAfee, 2022. [Online]. Available: https://www.mcafee.com

[5] Symantec, "What is a Trojan Horse? How It Works & How to Remove It," Broadcom, 2021. [Online]. Available: https://www.broadcom.com

[6] McAfee, "How to Detect and Remove Trojan Malware," McAfee, 2022. [Online]. Available: https://www.mcafee.com

[7] Federal Trade Commission (FTC), "What is Phishing?" FTC, 2023. [Online]. Available: https://www.consumer.ftc.gov/articles/phishing

[8] Federal Bureau of Investigation (FBI), "How to Protect Yourself from Vishing and Phishing," FBI, 2023. [Online]. Available: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/phishing

[9] StaySafeOnline, "Protect Yourself from Smishing Attacks," StaySafeOnline, 2023. [Online]. Available: https://www.staysafeonline.org

[10] Europol, "Ransomware: No More Ransom," Europol, 2021. [Online]. Available: https://www.europol.europa.eu

[11] Federal Trade Commission (FTC), "Mobile Malware and How to Protect Yourself," FTC, 2023. [Online]. Available: https://www.consumer.ftc.gov/articles/0022-mobile-malware

[12] StaySafeOnline, "How to Protect Your Mobile Device from Malware," StaySafeOnline, 2023. [Online]. Available: https://www.staysafeonline.org