The Dangers of Malware within the Puerto Rican Family Home: Threats, Impacts, and Preventive Measures

Author: Joseph R. González-Ríos
Advisor: Alfredo Cruz, Ph.D.
Master in Computer Science
Graduate Project EXPO, May 2026

Abstract

ZeroDay Tech Labs is a bilingual cybersecurity education platform for Puerto Rican family homes. The project addresses a practical gap: families rely on connected devices for daily life, but many lack simple guidance for recognizing and responding to malware, phishing, and privacy risks. The platform translates trusted cybersecurity guidance into plain-language learning paths, practical checklists, and controlled case studies. A pre use survey of 27 respondents shaped the design, while a post use survey of 20 respondents evaluated confidence, usefulness, and practical next steps. The result is an applied educational model that helps families pause, verify, act safely, and recover calmly.

Introduction

Puerto Rican families use phones, laptops, smart TVs, tablets, and shared accounts for banking, school, communication, entertainment, and family records. Because many security decisions happen quickly, the project focuses on practical household actions instead of technical theory alone.

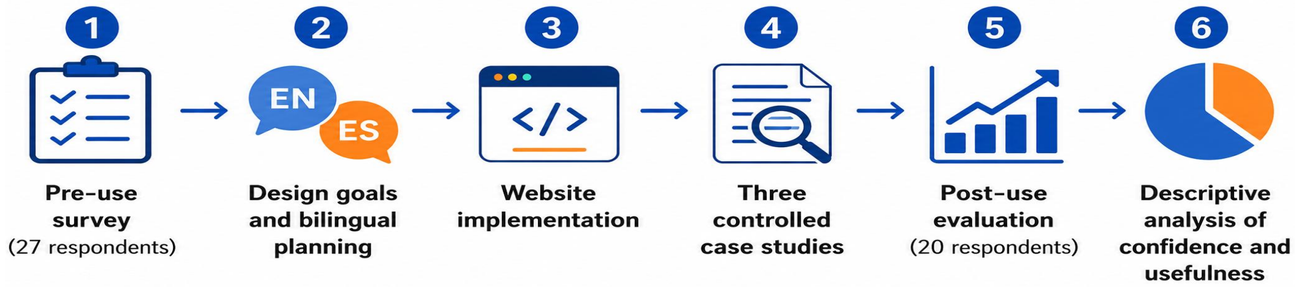
Background

The project is grounded in Protection Motivation Theory, which explains how people respond when they understand risk, believe action can help, and feel capable of acting. NIST CSF 2.0, CISA, NSA, and WCAG 2.2 guidance support the platform's focus on prevention, recovery, accessibility, and plain language cybersecurity education.

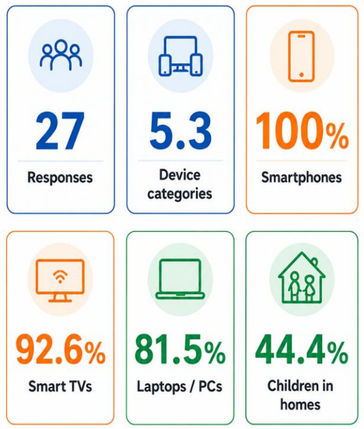
Problem

Household cyber risk often begins with ordinary actions: tapping a link, entering a password, approving an app, or allowing a browser prompt. Many families do not have a simple path for deciding what to do before, during, or after a mistake. ZeroDay Tech Labs addresses this problem by giving families bilingual guidance, checklists, case examples, and recovery steps they can use in real household situations.

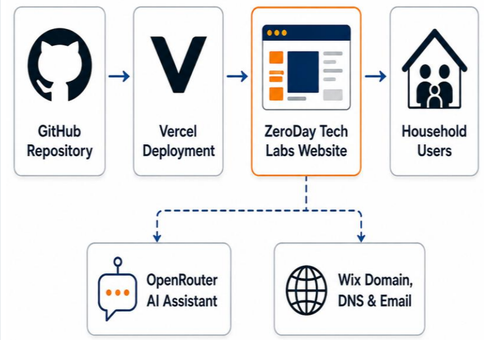
Methodology



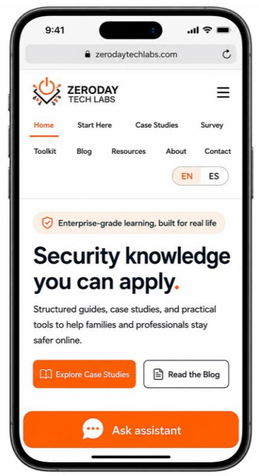
Evidence Snapshot



Current Deployment Stack

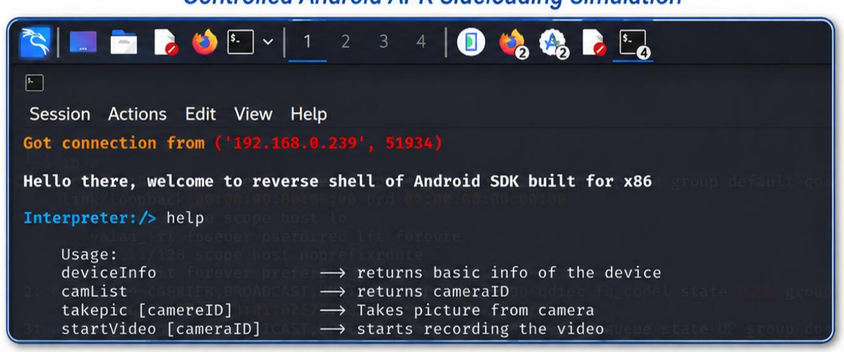


ZeroDay Tech Labs



Case studies

Controlled Android APK Sideloading Simulation



Main evidence for Case Study 2: reverse shell command view from the controlled Android APK sideloading simulation.

1 Case Study 1: Credential Exposure at the Point of Entry

Risk: Cloned login forms can capture submitted usernames and passwords.

Defensive takeaway: Verify the destination, use trusted bookmarks or passkeys, and change exposed passwords.

3 Case Study 3: Browser-Based Location Disclosure

Risk: Location prompts can reveal device and location data after permission is granted.

Defensive takeaway: Deny unexpected requests, verify the site origin, and review browser permissions.

Results and Discussion

Post use results showed increased confidence and practical action (20/20), with the Toolkit and controlled case studies rated as the most helpful learning components (18/20 each). The AI chat assistant was the least helpful component (13/20). These findings support a bilingual, mobile first approach to household cybersecurity education.

Conclusions

Household cybersecurity education is most effective when guidance is practical, accessible, and family centered. Scenario based learning helps users connect cybersecurity concepts to real world decisions, while bilingual educational resources can improve awareness, confidence, and safer online behavior within the home environment.

Future Work

Future work will focus on expanding evaluation through matched anonymous pre use and post use measurements, conducting usability testing with mixed age households, developing additional modules on SIM swap fraud, delivery scams, password managers, smart TV privacy, and cloud backup recovery, and continuing accessibility reviews and bilingual content improvements.

Acknowledgements

The author thanks Dr. Alfredo Cruz for guidance and mentorship, all survey participants for their time, and the Graduate School of the Polytechnic University of Puerto Rico for supporting this project.

References

[1] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," The Journal of Psychology, vol. 91, no. 1, pp. 93-114, 1975.
[2] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 2024. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29.
[3] Cybersecurity and Infrastructure Security Agency, Secure Our World. [Online]. Available: https://www.cisa.gov/secure-our-world.
[4] National Security Agency, Best Practices for Securing Your Home Network, Cybersecurity Information Sheet, 2023. [Online]. Available: https://www.nsa.gov/cybersecurity-guidance.
[5] World Wide Web Consortium, Web Content Accessibility Guidelines (WCAG) 2.2, 2024. [Online]. Available: https://www.w3.org/TR/WCAG22/.
[6] J. R. Gonzalez Rios, "Pre/Post-use survey responses," unpublished survey data, 2026.
[7] Federal Bureau of Investigation, Internet Crime Complaint Center, 2025 IC3 Annual Report, 2026. [Online]. Available: https://www.ic3.gov/annual report/reports.
[8] J. R. Gonzalez Rios, ZeroDay Tech Labs home, 2026. [Online]. Available: https://zerodaytechlabs.com.