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

Joseph R. González-Ríos
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, May 2026

Abstract *— This paper presents ZeroDay Tech Labs, a bilingual, cybersecurity education platform built for Puerto Rican family homes. The project responds to a practical problem: families depend on phones, laptops, smart televisions, cloud accounts, and online services, but many lack a simple way to recognize malware related risk and act before damage spreads. The platform translates trusted cybersecurity guidance into plain language learning paths, printable actions, and controlled case studies. A pre-use survey of 27 respondents shaped the household focus, while a post-use survey of 20 respondents evaluated confidence, useful components, and practical steps. The paper summarizes the project framework, website implementation, survey evidence, defensive case studies, privacy and accessibility choices, and limitations. The result is an applied educational model that helps families slow down, verify suspicious prompts, choose safer actions, and recover with less panic when cyber threats appear.*

Keywords *—Bilingual cybersecurity education, controlled case studies, household malware prevention, Puerto Rican homes.*

INTRODUCTION

Household cybersecurity is not simply a smaller version of business security. Businesses normally have administrators, procedures, inventories, patching schedules, and security budgets. Families usually rely on default settings, shared devices, informal advice, and urgent decisions made while someone is already worried. That difference matters. A parent, student, older adult, or home worker may need to judge a suspicious message, pop-up, app request, or login prompt without the support that an organization would have.

This paper summarizes the full project in the required university format. ZeroDay Tech Labs was implemented as a public, bilingual, mobile first platform that helps Puerto Rican family homes recognize common threats, make safer decisions, and recover calmly after mistakes. The paper highlights the problem, design evidence, platform implementation, attack profiles, controlled case studies, post-use evaluation, and limitations.

The project does not claim that a website can eliminate malware or fraud. Its claim is modest and practical: families can make better decisions when trusted guidance is translated into clear learning paths, visible examples, short checklists, and safe next steps. The goal is calm action, not fear.

PROBLEM AND FRAMEWORK

The central problem is the gap between household dependence on connected technology and household capacity to manage cyber risk. One phone may support banking, health appointments, school messages, family photos, password resets, and emergency communication. A smart television, game console, tablet, or home device may also share the same network. A household security mistake can therefore affect more than one device or account.

The project uses Protection Motivation Theory because household users need more than warnings. They need to understand that a threat is serious, believe that it can affect them, see that the recommended response can work, and feel capable of carrying out that response [1]. The NIST Cybersecurity Framework 2.0 also supports the design because its functions can be translated into household language: govern becomes family rules, identify becomes knowing important devices and accounts, protect becomes passwords, updates, and

backups, detect becomes recognizing suspicious prompts, respond becomes first steps after exposure, and recover becomes restoring access and trust [2].

Table 1 summarizes how CISA, NSA, and accessibility standards support the same direction: practical actions, safe home networks, phishing awareness, updates, multifactor authentication, and readable design for different users [3], [4], and [5].

Table 1
Project Focus, Evidence, and Paper Contribution

Focus area	Evidence used	Paper highlight
Household risk	Pre-use survey plus national threat guidance	Shows why a family home is a multi-device security environment.
Platform solution	Start Here, Toolkit, case studies, and resources	Explains how the website turns guidance into practical learning paths.
Technical depth	Three controlled case studies with redacted artifacts	Documents credential, app, and browser-permission decision points.
Evaluation	20 post-use responses	Shows perceived confidence, usefulness, and practical readiness.

Table 1 helps show that the paper is not built only on personal observation. It links official guidance with the project contribution, so the reader can see why household checklists, plain-language warnings, and accessible design belong in the cybersecurity solution rather than as extra website features.

Methodology

Figure 1 outlines the project workflow from survey input to evaluation. The method turns findings into design goals, builds the website resources, documents controlled case studies, and evaluates user perception through the post-use survey.

The pre-use survey included 27 respondents and served as design input for the platform [6]. The implementation phase produced the ZeroDay Tech Labs website, including Start Here, Toolkit, Case Studies, Resources, Blog, Survey, About, Contact, and supporting legal sections. The post-use survey included 20 respondents and measured perceived confidence, helpful components, and practical steps after platform use [7].

The case study phase used controlled simulations involving credential entry, mobile application installation, and browser-based location disclosure. Each study relied on researcher-controlled systems, redacted evidence, and self-generated or researcher-owned test artifacts. The paper discusses the cases at the level of risk, decision points, evidence, and mitigation rather than operational attack instructions.

Figure 1
Applied Project Workflow

Figure 1 keeps the project sequence visible. It clarifies that the website was not created first and justified later; the process moved from household need, to requirements, to implementation, to controlled case evidence, and finally to evaluation. That order supports the applied design logic of the paper.

Threat and Pre-Use Survey Evidence

The threat landscape supports a household-focused platform. The FBI Internet Crime Complaint Center reported high complaint volume and major financial losses, while phishing and spoofing remained a major complaint category [8]. These national indicators do not replace local household data, but they show that fraud, credential exposure, and social engineering are not fringe problems.

The pre-use survey confirmed that the target environment is a connected household ecosystem. Smartphones were reported by all 27 respondents, smart televisions by 25, laptops or desktops by 22, tablets and smart home devices by 18 each,

wearables by 16, and game consoles by 14 [6]. The average household selected 5.3 device categories. This supports an ecosystem approach rather than a single-device guide.

The family context also matters. Twelve of 27 respondents reported children under 18 in the household. That finding reinforces the need to support parents, caregivers, children, older adults, and nontechnical users instead of assuming one type of reader.

Figure 2 visualizes the pre-use survey evidence in a compact form. The figure highlights the number of pre-use respondents, average device categories, smartphone coverage, smart television use, laptop or desktop use, and households with children. It helps the reader quickly understand why the project treats the home as a connected environment rather than a single computer problem.

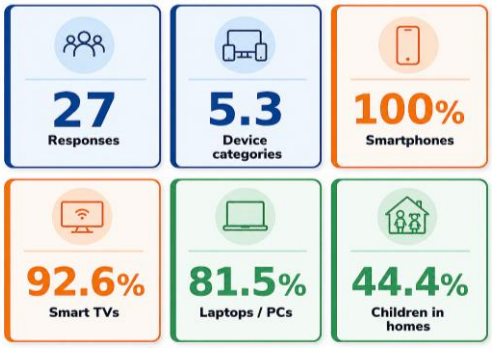

Figure 2
Pre-Use Household Evidence Snapshot

Table 2 explains the same pre-use evidence in a more organized way by connecting each survey signal to a design implication. This matters because the first survey shaped the platform before the website and case studies were finalized.

Together, Figure 2 and Table 2 clarify why the paper stays focused on ordinary household decisions before presenting the website and case study evidence. The pre-use data points to many devices, mixed-age users, and a need for practical steps. The visual summary gives the quick view, while the table gives the interpretation that supports the design choices.

Table 2
Pre-Use Evidence and Design Implications

Survey signal	Design meaning
Connected home	Multi-device environment.
Mobile risk	Strong mobile entry point.
Mixed-age audience	Family-readable lessons.
Design need	Checklists + scenarios

The pre-use evidence also explains why the platform avoids a single-device security approach. A Puerto Rican family home may include phones, smart televisions, laptops, tablets, wearables, game consoles, and shared accounts. Because one mistake can affect banking, school communication, photos, passwords, or recovery channels, the platform treats the home as an ecosystem rather than one isolated computer.

Platform Implementation and Deployment

ZeroDay Tech Labs organizes the learning experience around Start Here, Toolkit, Case Studies, Resources, Blog, Survey, About, Contact, and supporting legal or privacy content [9], [10], [11], [12]. The site is built to give first-time users a calm entry point and returning users a direct path to checklists, case studies, or resources.

The Start Here and Toolkit sections are more than supporting pages. Start Here gives first-time users a plain-language entry point before technical case studies, while the Toolkit gives families checklists and printable steps they can reuse during normal household routines [10], [11], [12]. Together, these sections convert official guidance into family behavior.

Figure 3 presents the mobile homepage from the user's perspective. The image removes annotation boxes so the reader sees what a first-time visitor would actually see on a phone: the brand, bilingual option, main navigation, Case Studies path, Toolkit access, Blog entry point, and assistant button. That perspective matters because the platform must be usable during ordinary household browsing, not only on a desktop screen.

The implementation also uses a low-friction privacy model. The initial learning flow does not require account creation, router passwords, incident screenshots, or sensitive uploads. Optional surveys gather evaluation data without turning the platform into a repository of private household security details.

This design choice also helps with trust. A family member is more likely to use a safety website when the first step does not ask for private incident details, screenshots, router passwords, or account information. The site can teach safer behavior while keeping the visitor in control of what they choose to share.

Figure 3
ZeroDay Tech Labs Mobile Homepage View

Figure 3 is included as webpage evidence rather than decoration. It illustrates that the first screen gives a family member several direct paths into learning and action before the user scrolls deeply into the site. That layout supports the project goal of guiding users from recognition to safer next steps without forcing them through technical wording first.

From a household perspective, the phone view is not only a layout choice. Many risky actions begin on the same type of screen: a text link opens in a browser, a prompt asks for location, a download button appears, or a user looks for help quickly. Showing the page in a mobile frame therefore connects the platform design to the way families actually encounter risk during normal browsing.

The deployment model also supports the project privacy goal. A static-first website reduces operational complexity and limits the need for user accounts or databases. Dynamic features can stay narrow: language switching, optional chat assistance, survey links, and future privacy-conscious analytics. The repository and website evidence also help the project remain verifiable because the written work is supported by a working implementation, not only a planning artifact [9], [10], [11], [12], [13].

Figure 4 maps the current deployment architecture for ZeroDay Tech Labs. The source code and educational assets are maintained in GitHub, Vercel publishes the static site and serverless API, OpenRouter supports optional assistant access, and Wix supports the public domain, DNS, and email identity. The figure matters because the technical stack affects privacy, maintainability, and user trust, not only the appearance of the website.

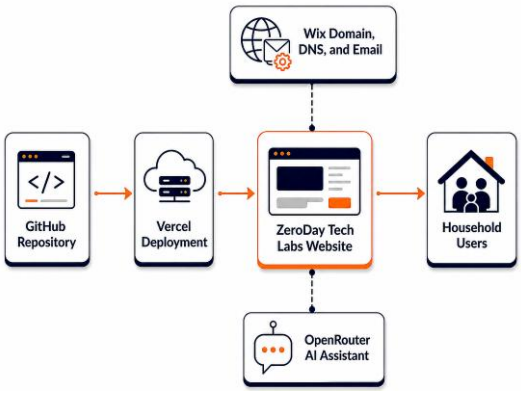

Figure 4
Current Deployment Stack

Figure 4 serves as implementation evidence, not decorative architecture. GitHub serves as the source-of-record for the website code, page structure, and educational assets. Vercel publishes the static site and serverless API, Wix supports the public domain, DNS, and email identity, and OpenRouter supports optional assistant access. Together, those layers show how the platform can remain public and usable while keeping dynamic behavior narrow.

The practical deployment value is that most learning content can remain static and public while the assistant and survey paths stay optional. That separation reduces the need for databases, passwords, private household uploads, or account creation. It also makes the project easier to maintain because updates can be made in the repository, redeployed through the same pipeline, and accessed by families without changing the privacy posture of the site.

Together, Figure 3 and Figure 4 make clear that ZeroDay Tech Labs is not only a written proposal. Figure 3 presents the visitor-facing mobile experience, while Figure 4 maps the deployment path that supports it. The result is a working public implementation where design, code, domain support, deployment, and optional assistance all support the same educational purpose: deliver practical guidance to households without collecting more data than necessary.

Attack Profiles and Case Studies

General scam and phishing guidance support the phishing and credential-risk framing, while the remaining household examples in Table 3 are presented as defensive patterns rather than separate source-heavy claims [14], [15].

That point matters because malware-related harm often begins before malware is installed. A fake message can steal credentials, a call can persuade someone to reveal a code, a text link can lead to a fake payment page, a believable story can collect recovery details, and a scareware pop-up can push a person to install unwanted software or allow remote access. Table 3 condenses the common lesson: slow down, verify through a trusted path, and recover quickly if exposure occurs.

Table 3 acts as the bridge between threat awareness and household action. It does not teach the reader how to perform attacks. Instead, it reduces each profile to the visible pressure point, the risky choice, and the safer response. That keeps the discussion defensive and consistent with the family-centered purpose of the project.

The controlled case studies add technical depth without shifting the paper into an attack manual. Each one centers on a small household decision point: submitting a form, approving an app, or allowing a browser prompt. Case Study 1 documents credential exposure at form submission inside a localhost simulation. Case Study 2 explains how an untrusted APK becomes risky only after the user approves installation and opens it. Case Study 3 demonstrates that location and device context can be disclosed after a browser permission prompt, even when no password is typed, and no malware is installed [9].

Table 3
Household Attack Profile Highlights

Profile	What the household sees	Defensive highlight
Phishing	Fake email, payment notice, or login page	Verify through the real app or typed website; use MFA.
Vishing	Urgent call from a bank, agency, or support line	Hang up and call back using a trusted number.
Smishing	Text link about delivery, tolls, or account alerts	Do not tap surprise links; open the official app.
Pretexting	Believable story using family, school, or authority	Verify with a known contact before sharing details.
Scareware	Fake infection warning or support pop-up	Close the browser and use trusted support paths.

The purpose is to identify what a normal family member would notice at the screen level. In each scenario, the safe response is simple enough to remember during stress: stop the action, verify the source through a trusted path, remove questionable access, and change credentials if exposure is possible. This keeps the case studies useful for families while still giving the paper technical evidence.

Table 4 summarizes these controlled scenarios as defensive learning points. The table identifies the risk moment, the household decision, and the lesson that should be remembered after viewing the evidence. It also helps the reader compare the three cases without turning the section into a tool walkthrough. Because the scenarios are controlled, the table also protects the ethical boundary of the paper: the reader sees what was learned, but the

presentation stays focused on recognition, prevention, and recovery rather than attack steps.

The controlled case studies stay within a defensive purpose, not operational instruction. Each scenario uses bounded evidence, redacted artifacts, and researcher-controlled resources so the reader can understand the decision point without receiving an attack walkthrough. This keeps the technical depth aligned with the project's ethical purpose.

Table 4

Controlled Case Study Matrix and Defensive Learning

Case study	Risk moment	Defensive learning
Credential exposure	Login form captures test credentials at submission.	Verify URL; use MFA or passkeys; rotate exposed passwords.
Mobile app entry	Untrusted APK becomes risky after install approval.	Avoid side loading; use trusted stores; review app permissions.
Location disclosure	Browser prompt exposes location and device context.	Deny surprise prompts; review saved permissions; verify need.

Figure 5 captures the credential harvester evidence from the controlled localhost simulation. The purpose of the figure is to identify the exact decision point where exposure occurs: the user submits a form that appears familiar, and the submitted information is captured in the lab environment.

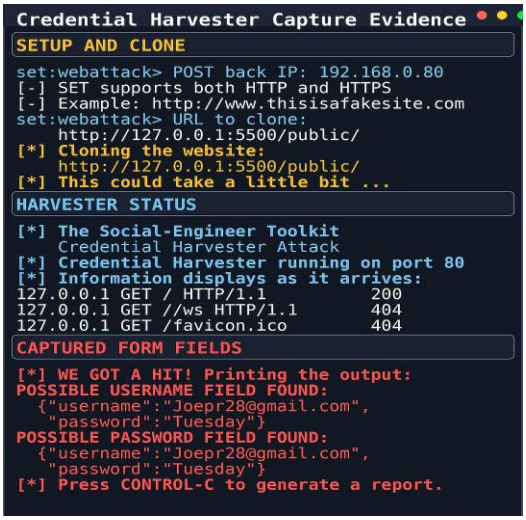

Figure 5

Credential Harvester Capture Evidence

Figure 5 serves as defensive evidence. It demonstrates why a household user cannot rely on appearance alone when entering credentials. The safer habit is to use trusted bookmarks, official apps, password managers, or passkeys so the destination is verified before the form is submitted.

Figure 6 documents the Android reverse shell command view from the controlled mobile simulation. It supports the defensive lesson that the risky moment is not only downloading a file; the larger risk begins when the user approves the installation, opens the application, and treats the activity as normal.

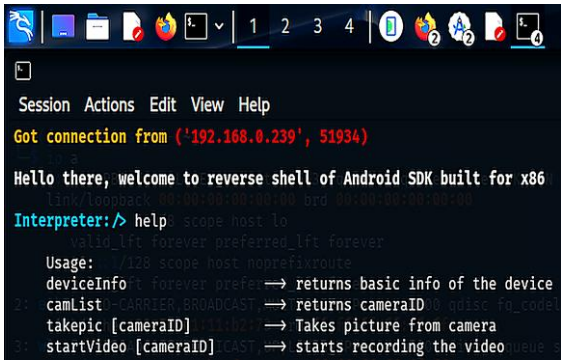

Figure 6

Android Reverse Shell Command View

Figure 6 works as the mobile device evidence for the second case study. It reinforces the lesson that the household defense happens before execution: avoid untrusted application packages, keep installation sources restricted, review permissions, and remove suspicious applications quickly when something looks wrong.

Figure 7 illustrates the browser location permission prompt. This figure demonstrates that privacy exposure can begin with an ordinary browser request when the user does not verify the page first. The lesson is simple for households: a permission prompt is a trust decision, not background noise.

Figure 7 serves as the privacy-decision evidence for the third case study. The prompt looks normal, but the decision still matters. A family member who denies unexpected location requests and reviews saved browser permissions reduces exposure without needing advanced technical knowledge.

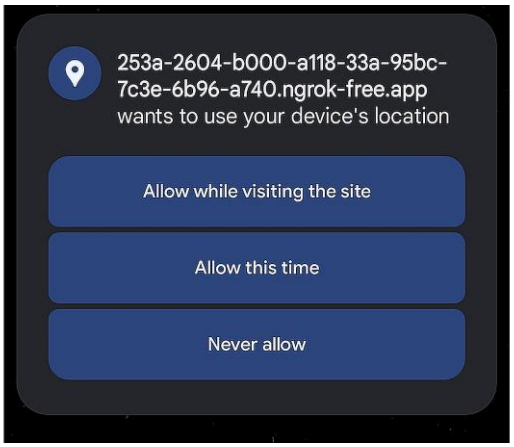

Figure 7
Browser Location Permission Prompt

As a set, Figure 5, Figure 6, and Figure 7 demonstrate that the critical security moment is usually a normal user decision, not a dramatic technical event. The user types into a form, opens an app, or approves a browser prompt. That pattern makes the case studies useful for family education because the safer response can be taught as a repeatable habit: pause, verify, deny unexpected access, and recover through trusted paths.

Evaluation and Discussion

The evaluation is descriptive and applied. It does not claim a causal experiment because pre-use and post-use responses were not linked at the individual level. Instead, the evaluation asks whether users reported confidence, practical usefulness, and helpful learning components after interacting with the platform.

The clearest result is confidence. All 20 post-use respondents reported being either more confident or much more confident after using the website [7]. That confidence result matters because household users who feel incapable often delay security action. The goal is not overconfidence; the goal is informed self-efficacy supported by practical steps.

The practical action result is also strong. Seventeen respondents answered yes and three answered somewhat when asked whether the site provided practical steps they could apply to protect themselves or their household [7]. Toolkit and case studies were each selected by 18 of 20 respondents as helpful components, which supports the project design choice: combine simple checklists with scenario-based evidence.

Figure 8 presents the post-use evaluation highlights. The figure gives the reader a quick view of confidence, practical steps, Toolkit usefulness, case study usefulness, general information usefulness, and chat assistant usefulness. It is included because the visual comparison makes the strongest post-use results easy to see.

Figure 8
Post-Use Evaluation Highlights

Figure 8 remains the evaluation visual because it presents the post-use pattern more clearly than a second table. All 20 respondents reported increased confidence, 17 answered yes and 3 answered somewhat for practical steps, and the Toolkit and case studies were each selected by 18 respondents as helpful components [7]. These results indicate that users did not only read the site; they recognized actions they could apply in the home.

The post-use results should still be read as practical user feedback rather than causal proof. The pre-use and post-use responses were not linked at the individual level, and the sample is exploratory. Within that scope, the pattern supports the platform design: users valued the action-oriented Toolkit, scenario-based case studies, and general guidance because those components helped turn cybersecurity information into everyday household steps.

Viewed as a whole, the results support ZeroDay Tech Labs as an applied household cybersecurity education intervention. The pre-use survey explains why the platform needs to be broad, bilingual, and mobile-first. The case studies explain why decision

points matter. The post-use survey suggests that users found the platform understandable, useful, and confidence-building within the limits of the study design.

The evaluation also reinforces the reason for using both checklists and case evidence. The Toolkit gives users direct actions, while the case studies explain why those actions matter at the moment of risk. This pairing is stronger than awareness alone because it connects information to behavior.

Privacy and Accessibility

Privacy and safety by design are built into the educational model. The platform should not require users to create accounts, share router credentials, upload sensitive screenshots, or describe private incidents in detail. Survey collection should remain aggregate and low risk. The case studies follow the same principle by using controlled environments, redacted artifacts, localhost scope, virtual devices, and researcher-owned systems.

Accessibility is also a security requirement. If older adults cannot read the page, mobile users cannot navigate it, or bilingual users receive uneven content, the platform will not reduce risk. WCAG 2.2 supports readable contrast, meaningful links, keyboard access, alt text, and language parity [5]. The Start Here and Toolkit sections translate that accessibility principle into practical household learning.

This is a practical security issue, not a design extra. A family member who cannot read a warning clearly, understand a bilingual label, or find the next safe step may still make the risky choice even if the information exists somewhere on the page. Accessibility therefore supports prevention because it keeps the protective instruction usable at the moment the user needs it.

Bilingual presentation supports the same goal. When English and Spanish pages use the same structure, families do not have to treat one language as the complete version and the other as a shortcut. That consistency is important in Puerto Rican households where family members may switch languages when helping each other with phones, accounts, and suspicious messages.

Safety by design also includes emotional safety. Household users may delay action if they feel embarrassed, blamed, or technically incapable. The platform should therefore explain recovery calmly and avoid shame-based language so families are more willing to ask for help after a mistake.

Limitations and Future Work

The project has limitations that should remain visible in the paper. The pre-use survey used 27 respondents and the post-use survey used 20 respondents, so the findings are useful for design and exploratory evaluation but not for population-level generalization. Some pre-use items had smaller valid response counts because the instrument evolved during collection [6].

The post-use data rely on self-report and are not linked to individual pre-use responses. This protects privacy and reduces friction, but it prevents paired statistical analysis. Future work should use an anonymous code system that allows matched pre-use and post-use comparison without collecting names or sensitive identifiers.

The next phase should include usability testing with mixed age households, follow up checks on practical behavior, expanded modules on SIM swap risk, fake delivery messages, password manager setup, smart television privacy, cloud backup recovery, and reporting resources. A maintenance calendar should also be kept: monthly link checks, quarterly bilingual parity reviews, quarterly accessibility checks, and annual framework alignment reviews.

Future work should also focus on stronger evaluation and broader household testing. An anonymous code system could allow matched pre-use and post-use comparison without collecting names, while mixed-age usability sessions with parents, caregivers, older adults, and teens would help improve wording, navigation, and Toolkit design before wider community use.

Conclusion

ZeroDay Tech Labs demonstrates that a bilingual cybersecurity education platform can make

household malware prevention more understandable and actionable. It starts with a real family-centered gap, uses survey input to define needs, implements a public website, documents safe case studies, and evaluates whether visitors leave with more confidence and usable steps.

The strongest contribution is the connection between scenario-based learning and practical action. Families do not need to memorize every technical term before becoming safer. They need to recognize pressure, verify before acting, avoid untrusted downloads, protect accounts, deny unexpected prompts, and recover calmly after mistakes.

Within its exploratory scope, the project is strong because it is implemented, evidence-informed, ethically bounded, and focused on the people named in the title: Puerto Rican families. The paper, therefore, presents ZeroDay Tech Labs not as an abstract idea, but as a working educational bridge between official guidance and everyday household action.

REFERENCES

[1] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," in *The Journal of Psychology*, vol. 91, no. 1, pp. 93-114, 1975.

[2] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* [Online]. Available: https://doi.org/10.6028/ NIST.CSWP.29.

[3] Cybersecurity and Infrastructure Security Agency. (n. d.). *Secure Our World* [Online]. Available: https://www.cisa.gov/ secure-our-world.

[4] National Security Agency. (2023). *Best Practices for Securing Your Home Network, Cybersecurity Information Sheet* [Online]. Available: https://www.nsa.gov/ cybersecurity-guidance.

[5] World Wide Web Consortium. (2024). *Web Content Accessibility Guidelines (WCAG) 2.2* [Online]. Available: https://www.w3.org/TR/WCAG22/.

[6] J. R. González Ríos, "Pre-use survey results," unpublished survey data, 2026.

[7] J. R. González Ríos, "Post-use survey responses: Encuesta posterior al uso," unpublished survey data, 2026.

[8] Federal Bureau of Investigation. (2026). *Internet Crime Complaint Center, 2025 IC3 Annual Report* [Online]. Available: https://www.ic3.gov/annualreport/reports.

[9] J. R. González Ríos. (2026). *ZeroDay Tech Labs case studies* [Online]. Available: https://zerodaytechlabs.com/labs/.

[10] J. R. González Ríos. (2026). *ZeroDay Tech Labs home* [Online]. Available: https://zerodaytechlabs.com.

[11] J. R. González Ríos. (2026). ZeroDay Tech Labs Start Here [Online]. Available: https://zerodaytechlabs.com/start-here/.

[12] J. R. González Ríos. (2026). *ZeroDay Tech Labs ToolKit* [Online]. Available: https://zerodaytechlabs.com/toolkit/.

[13] J. R. González Ríos. (2026). *ZeroDayTechLabs source repository, GitHub* [Online]. Available: https://github.com/ Jectes/Zerodaytechlabs.

[14] Federal Trade Commission. (2023, July). *How to avoid a scam* [Online]. Available: https://consumer.ftc.gov/ articles/how-avoid-scam.

[15] Cybersecurity and Infrastructure Security Agency. (n. d.). *Recognize and Report Phishing* [Online]. Available: https://www.cisa.gov/secure-our-world/recognize-and-report-phishing.