

FLORIDA INTERNATIONAL UNIVERSITY



PHISHING DETECTION IN CHROME EXTENSION

Students: Juan Azcuna, Aiyanna Ferguson, Ivan Ortiz

Instructor/Faculty: Masoud Sadjadi , Florida International University

INTRODUCTION

PROBLEM

Cybercrime is at an all-time high and many online users are becoming victims of malicious activity. Phishing - the use of disguise to convince users to expose sensitive data about themselves or an organization- stands as the most common social engineering tactic used today. This demonstrates the need to develop resources capable of alerting online user of and protecting them from malicious activity.

Despite the decrease of phishing incident reports in the first quarter of 2024 compared to those reported in 2023, security measures are still needed to protect individuals and companies from the manipulation and malicious tactics of phishers.



Figure 1 Showing: A comparison between phishing incidents reported in the first quarter of 2023, and that which was reported in 2024.

INTRODUCTION

OBJECTIVE

The aim of this research project is to provide online users with a Chrome extension with the ability to analyze email content and embedded links within Gmail. Extensions enable users to add an additional layer of functionalities to their webpage.

With PhishGuard, users have the ability to determine the likelihood of emails in their inbox being phishing attempts by generating a careful, accurate analysis using Google built-in-AI. With this solution, we aim to contribute to the decreasing rate of phishing by alerting users of the safety of their emails.

This PowerPoint slide deck will provide an overview of the main components of the PhishGuard Chrome extension.

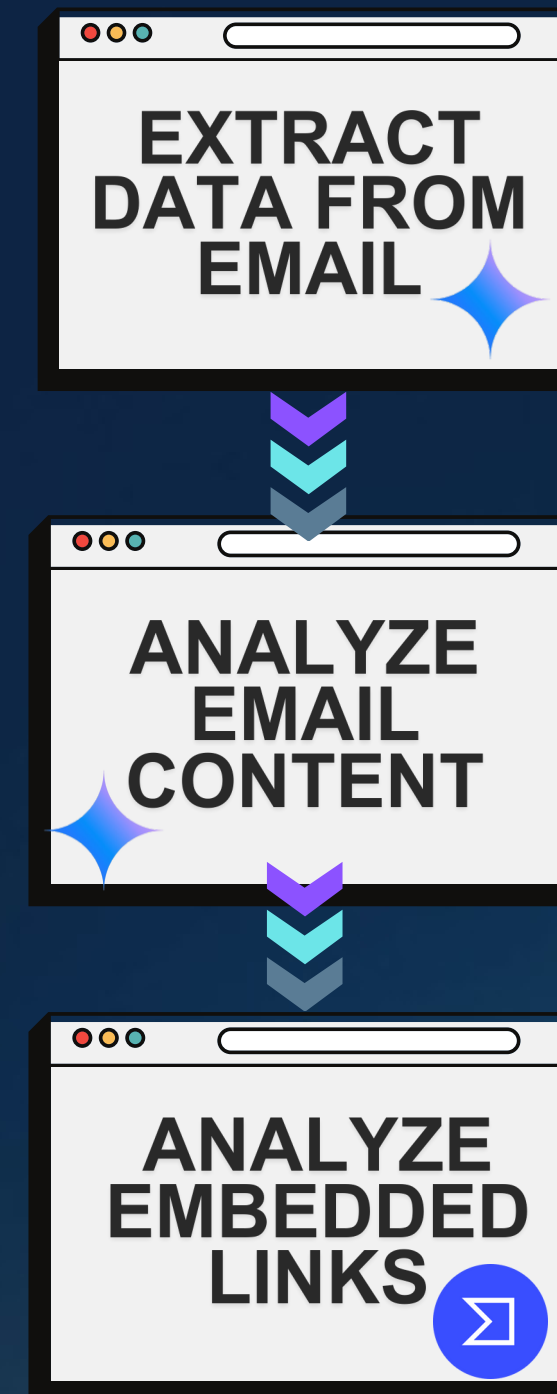


Figure 2 Showing: PhishGuard Project Overview

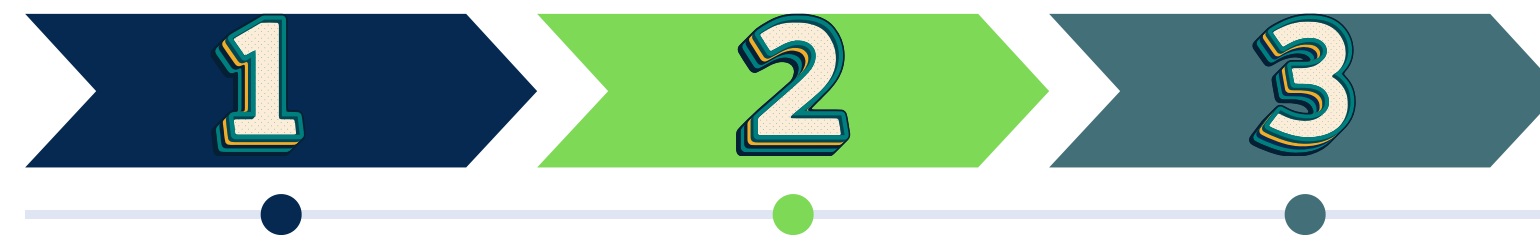




EMAIL CONTENT ANALYSIS



HOW IT WORKS



STEP 1: EXTRACT DATA

In order for the extension to analyze the data, it has to first extract it. A content script was created with the ability to extract the:

- 1 SENDER EMAIL ADDRESS
- 2 SUBJECT LINE
- 3 TIMESTAMP
- 4 EMAIL BODY

All of these components aid the user in determining whether or not the email was sent from a trusted source.

```
if (processedEmails.has(emailId)) {
  console.log('Email already processed:', emailId);
  return;
}

try {
  // Extract sender (using email attribute)
  const senderElement = emailContainer.querySelector('.gD');
  const sender = senderElement ? senderElement.getAttribute('email') : null;
  console.log('Found sender:', sender);

  // Extract subject
  const subjectElement = document.querySelector('h2.hp');
  const subject = subjectElement ? cleanText(subjectElement.textContent) : null;
  console.log('Found subject:', subject);

  // Extract body
  const bodyElement = emailContainer.querySelector('.a3s.a1l');
  const body = bodyElement ? extractStructuredBody(bodyElement) : null;
  console.log('Found body:', body ? `Yes (length: ${body.mainText.length})` : 'No');

  // Extract timestamp
  const timestampElement = emailContainer.querySelector('.g3');
  const timestamp = timestampElement ? timestampElement.getAttribute('title') : new Date().toISOString();
}
```

Figure 3 Showing: Snippet of Content.js Code



STEP 2: CALCULATE PHISHING SCORE

Once the data is extracted, it is sent to the service worker of the extension which manages the background processes and coordinates the analysis. The email is then analyzed by providing a well-defined prompt to the built-in Gemini model that assesses whether or not phishing indicators are present.

Consider these factors:

- Urgency or pressure tactics
- Grammar and spelling errors
- Suspicious links or attachments
- Requests for sensitive information
- Mismatched or fake sender addresses
- Time sent (suspicious if outside business hours)
- Sender legitimacy and domain analysis

Figure 4 Showing: Common Phishing Indicators considered by PhishGuard

```
async calculateScore(emailContent) {  
  try {  
    // Log emailContent for debugging  
    console.log('Email content received:', emailContent);  
  
    const features = this.analyzeEmailFeatures(emailContent);  
  
    // Check if the language model is available  
    const capabilities = await ai.languageModel.capabilities();  
  
    if (capabilities.available !== "readily") {  
      console.warn('Language model is not readily available');  
    }  
  
    if (capabilities.consent === "granted") {  
      console.log('Consent already granted.');
```

Figure 5 Showing: Code Snippet from phishing.js Script

STEP 3: ALERT USER

Once Gemini assesses the email using the phishing indicators shown in Figure 4, a phishing score is provided to the user, along with the email details gathered from the extraction.

Two additional options are also provided to users, one that allows them to directly access Google Safe Browsing 'Report Phishing' page, and the other that redirects them to PhishGuard GitHub page so that they can learn more.

User behavior is particularly important in cybersecurity because it can determine whether information is kept safe or eventually exposed to risk. Malicious actors can easily manipulate users, making them an easy target for phishing (Moustafa et al.).

Providing users with the phishing score and additional information about their email can help them make more informed decisions about which emails to interact with.

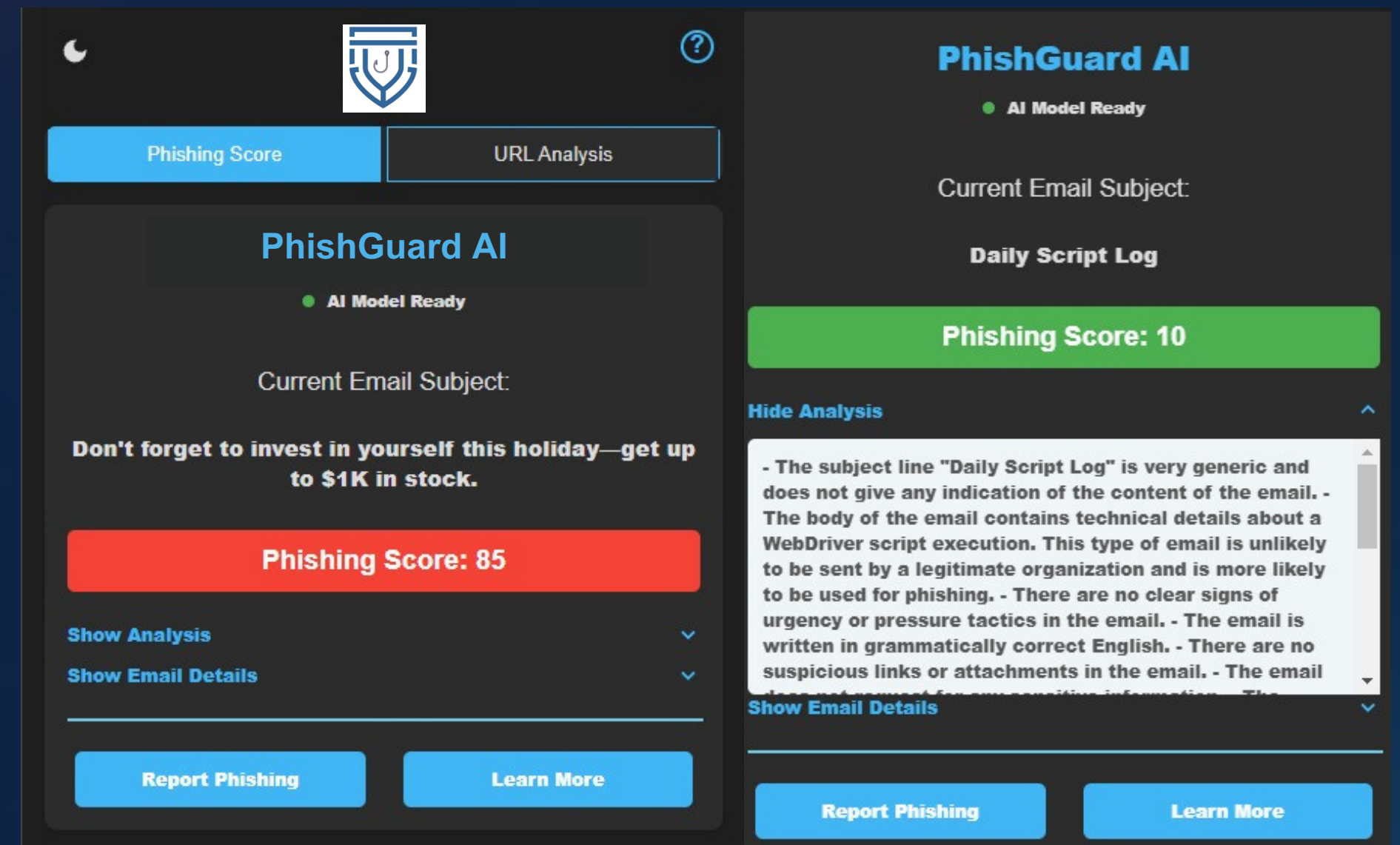
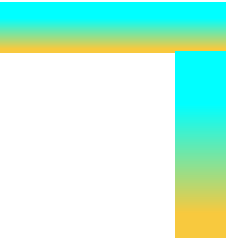
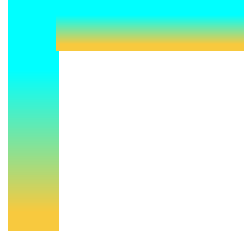
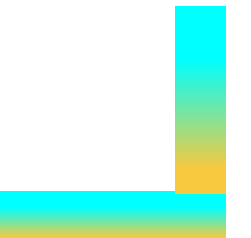
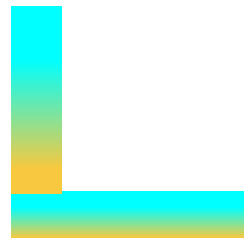


Figure 6 Showing: Difference between Popup Interface with a High Phishing Score & Low Phishing Score



LINK ANALYSIS FEATURE



PURPOSE

Over 90% of cybersecurity attacks begin with spear phishing emails (Varshney et al., 2024), and 46.6% of incident reports for the first and second quarter of 2024 shows webmail as one of the main target areas. In cases like this, phishers aim to alter the URLs (Uniform Resource Locator) present in emails to redirect users to malicious sites.

PhishGuard aims to combat this through its link analysis feature that gives users the ability to scan links within their email to determine their safety of the URLs (destination).



HOW IT WORKS



TRIGGER LINK ANALYSIS



RETRIEVE LINK & ANALYZE URL



ALERT USER

TRIGGER LINK ANALYSIS

Users are provided with 2 options to analyze the link:

1. A right-click option where they can right click the link and select 'Analyze Link' from the menu.
2. A pop-up interface where they can enter the link where they can paste the link and click 'Analyze Link'.

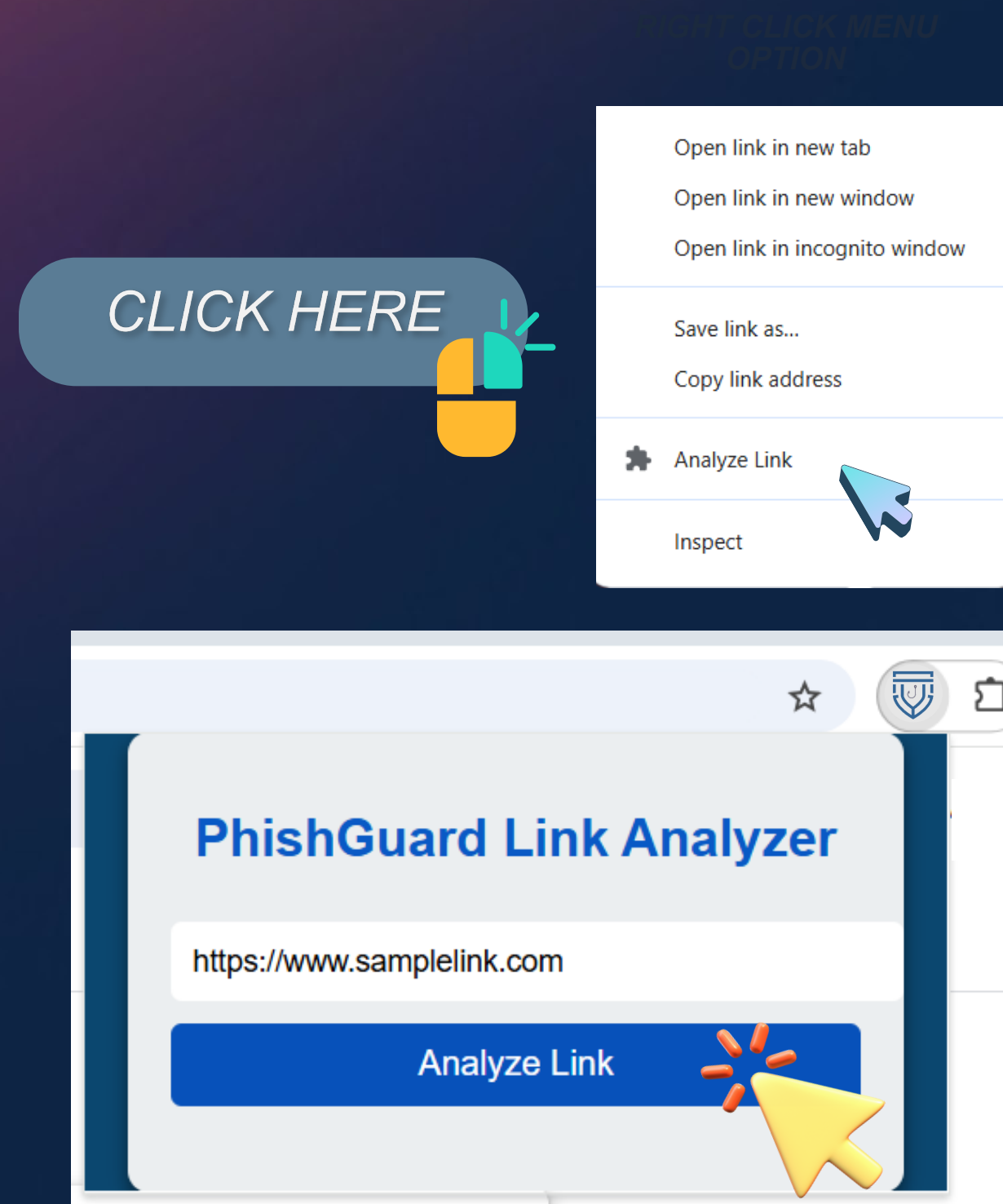


Figure 7 Showing: Link Analysis Options for Users

RETRIEVE LINK & ANALYZE URL



The background script will listen out for when the user clicks on the context menu item, and the popup script will send the request for the URL to be analyzed.

The background script will use the API key and the link received by the user to analyze the URLs by forwarding scan requests to VirusTotal v3 public API (Application Programming Interface). This process will occur in adherence to the limit of 4 requests per minute.

The background script will then fetch the scan report of the URLs provided by VirusTotal v3 public API and evaluate the safety of the URL.

```
function evaluateUrlSafety(report)
{
    if(!report) return {isMalicious: false, positives: 0, total: 0};

    const{positives, total} = report.stats_from_last_analysis;

    const isMalicious = positives > total / 2;

    return {isMalicious, positives, total};
}
```

Figure 8 Showing: Code Snippet of background.js Script for Link Analysis

PhishGuard will get the total amount of reports found for the submitted URL and determine how many of them are positives.

If no report is found, the link will be deemed safe, but if multiple reports are found and more than 50% of them are positive (indicates an unsafe link), the user will be notified.

ALERT THE USER

Once PhishGuard has evaluated the safety of the link, a message will be displayed on the popup. This feature, combined with the phishing score allows users to practice more online safety using Gmail.

```
if(response)
{
    if(response.status === "success")
    {
        const message = response.result.isMalicious
        ? `Warning: This link is unsafe. ${response.result.positives}/${response.result.total} scanners has detected malicious activity.`
        : "This link appears safe. You may proceed.";

        document.getElementById("result").textContent = message;
    } else
```

Figure 9 Showing: Code Snippet of popup.js Script for Response Handling

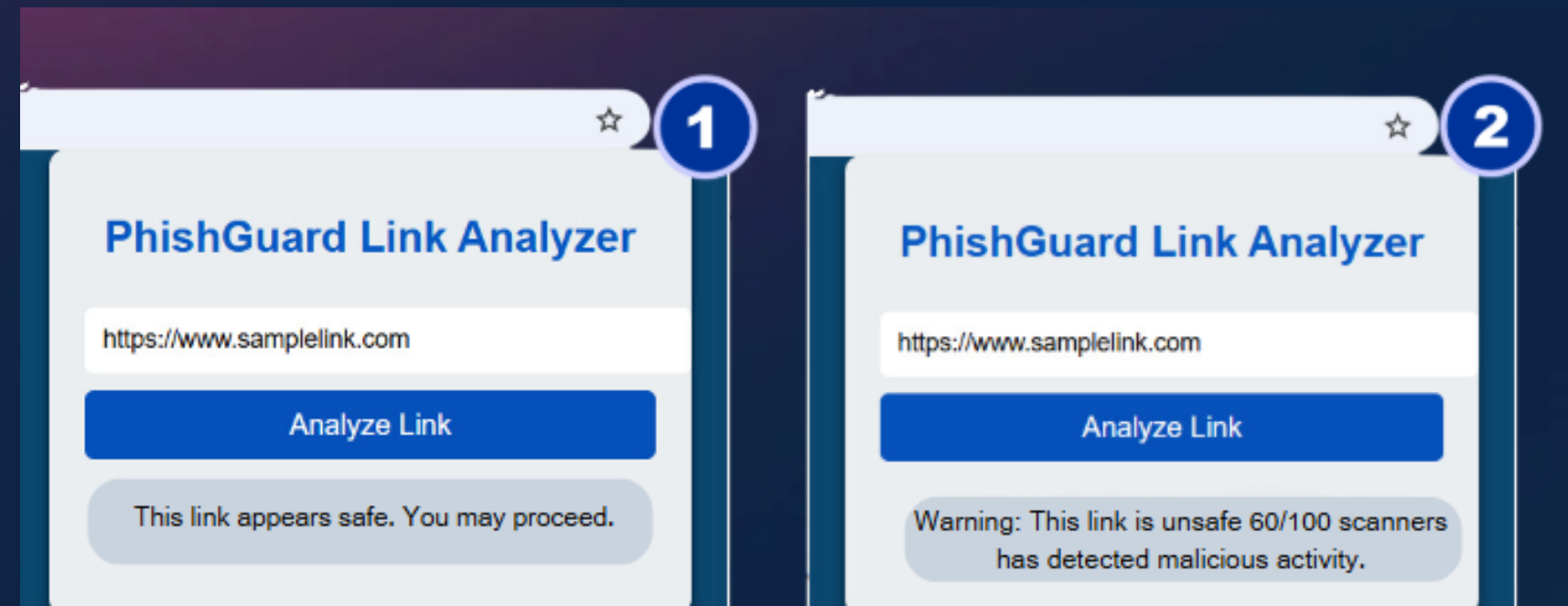
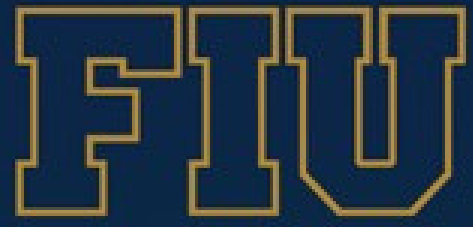


Figure 10 Showing: Desired Outcome for User Alerts



USER INTERFACE DESIGN

WHY IS IT IMPORTANT & HOW DOES IT RELATE TO PHISHGUARD

Users value their experience more with products when the quality of the user interface design is well-defined. Certain elements like the ease of use, and product appearance has a direct impact on user satisfaction (Qi and Xu). These elements also impact how brand authenticity is perceived (Wang et al.). PhishGuard incorporates these elements through the simplicity of its logo design and the presentation of the user interfaces.



```
.explanation {
  background-color: var(--background);
  padding: 15px;
  margin-top: 10px;
  border-radius: 5px;
  font-size: 0.9em;
  line-height: 1.4;
  color: var(--text-color);
  max-height: 200px;
  overflow-y: auto;
}

.toggle-explanation {
  color: var(--blue);
  cursor: pointer;
  display: flex;
  align-items: center;
  margin-top: 10px;
  user-select: none;
}

#analyzeButton {
  width: 100%;
  padding: 10px;
  background-color: #0751ba;
  border: none;
  color: white;
  font-size: 16px;
  border-radius: 5px;
  cursor: pointer;
}
```

Figure 12 Showing: Code Snippets from popup.html and popup.css scripts

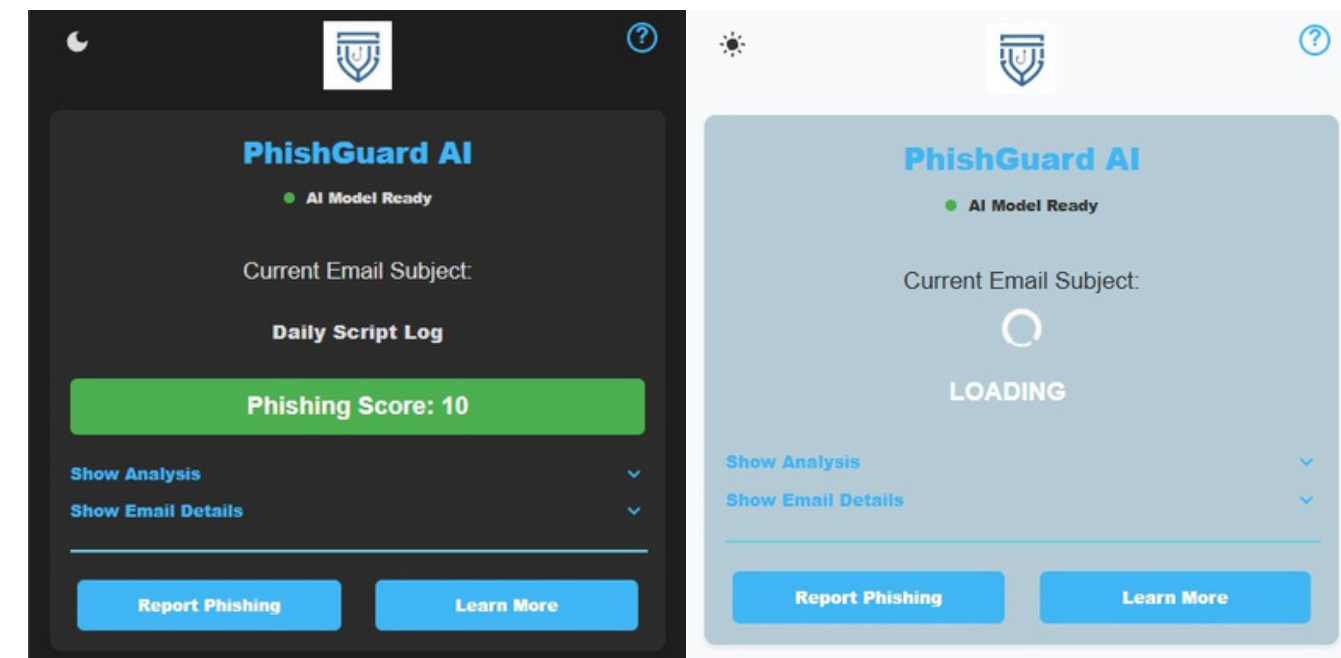


Figure 13 Showing: User Interface in Dark Mode and Light Mode

It is important to consider the risks that can be associated with the development or use of PhishGuard. With that, we have provided a risk analysis chart, highlighting the risks that may threaten the safety and efficiency the extension. We have also provided a risk matrix that highlights the severity and likelihood of each vulnerability.



Figure 14 Showing: Risk Assessment Table & Risk Matrix

TOOLS



REFERENCES

- "Phishing Activity Trends Report 1st Quarter 2023." APWG, 2 Nov. 2023.
- "Phishing Activity Trends Report 1st Quarter 2024." APWG, 14 May 2024.
- Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U., & Gupta, C. (2024). Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, 238, 122199. <https://doi.org/10.1016/j.eswa.2023.122199>
- Moustafa, Ahmed A., et al. "The Role of User Behaviour in Improving Cyber Security Management." *Frontiers in Psychology*, vol. 12, no. 12, 18 June 2021, <https://doi.org/10.3389/fpsyg.2021.561011>.
- "Phishing Activity Trends Report 2nd Quarter 2024." APWG, 21 Aug. 2024.
- Qi, Yan, and Rui Xu. "Research on User Interface Design and Interaction Experience: A Case Study from "Duolingo" Platform." *ICST Transactions on Scalable Information Systems*, 4 Apr. 2024. ResearchGate, www.researchgate.net/publication/379578564_Research_on_User_Interface_Design_and_Interaction_Experience_A_Case_Study_from_Duolingo_Platform, <https://doi.org/10.4108/eetsis.5461>.
- Wang, Yan, et al. "Simple = Authentic: The Effect of Visually Simple Package Design on Perceived Brand Authenticity and Brand Choice." *Journal of Business Research*, vol. 166, 1 Nov. 2023, p. 114078. *ScienceDirect*, www.sciencedirect.com/science/article/abs/pii/S0148296323004368, <https://doi.org/10.1016/j.jbusres.2023.114078>.

FLORIDA INTERNATIONAL UNIVERSITY



THANK YOU