



Phishing Detection in Chrome Extension

Fall 2024 Capstone Project
Students: Ivan Ortiz, Aiyanna Ferguson, Juan Azcuna
Instructor/Faculty: *Masoud Sadjadi*, Florida International University

Problem

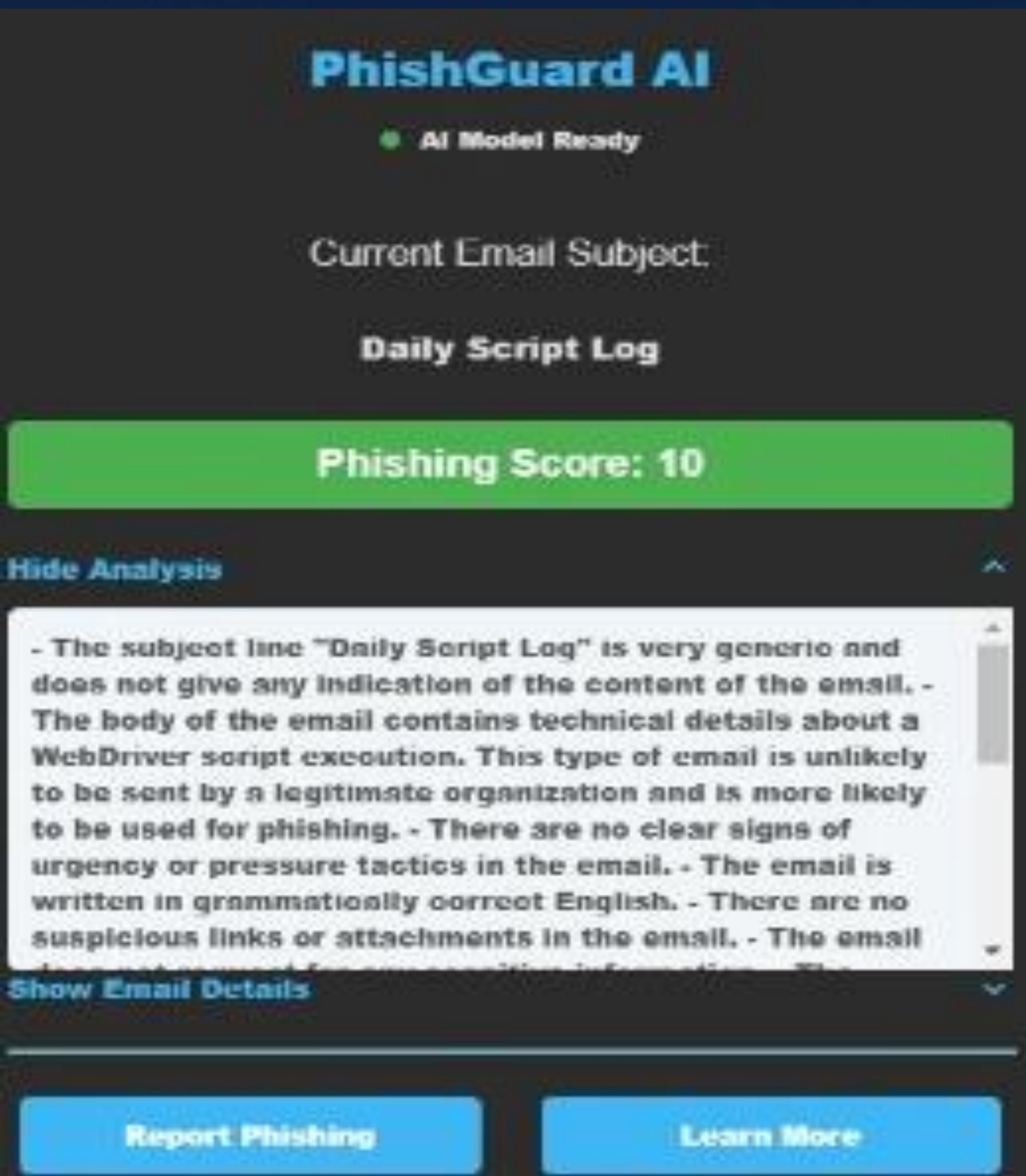
Phishing is a social tactic that tricks and deceives the user on the receiving end to give private information about themselves or others that they know of. It has been an ever-increasing problem since the public access to the Internet. It is very easy to fall to this scheme as it presents itself as an unassuming link that a regular web user could receive daily and instead takes them to an unsafe site.

Objective

Our extension will give the user a proper lenses to see what these phishing tactics for what they really are. It will give the user a helping hand by examining whatever incoming email they receive thru Gmail to view if the email contains any suspicious material inside that they wouldn't normally receive. The visual on the right simplifies how the extension will work in real time.

Requirements

- An API
- Coding knowledge in JavaScript, HTML, CSS and basic knowledge of Email/Gmail usage
- Data repository for all coding to go into, such as GitHub



Process

- Step 1: Extract all email data from the recipient
- Step 2: Wait for the extension to process the email data and see if there's any phishing activity present
- Step 3: Phishing score will provide how safe or dangerous the email link is to the user, and whether they wish to report this incident and/or learn more about what could have befallen them.

My portion

I was in charge of designing the logo for the Chrome Extension, which began with crude drawings of combining the Chrome logo with a bank vault to having the Chrome logo be the bank vault like the previous Google Authenticator logo to having it look like a logo created at the start of the project, which was a shield that had a hook design in the centerpiece.

