Project Plan - PhishGuard

Authors: Roko Mladinić, Daniella Namuli, Simeon Markov & Zed Minabowan

Table of contents

Introduction

Commented [MS1]: @Markov,Simeon S.

The purpose of this document is to present a clear overview of the project's idea, the problem that it focuses on resolving, the challenge that is imposed on, and the given solution. Moreover, it details the research, design, development, and testing phase of the project, breaking down steps, and reporting a clear plan.

Project overview

Commented [ND2]: @Namuli,Daniella D. responsible for this part

PhishGaurd is a web-based cybersecurity training tool designed to improve users' ability to recognize and respond to common cyber threats and tracks user performance data to identify weak spots.

While many organizations provide cybersecurity awareness training, they are often delivered through static materials such as PDFs, videos or presentations which often result in low engagement and poor knowledge retention, because users are not actively involved in the learning process hence remaining vulnerable to cyber threats. Additionally, organizations often lack insight into how well users understand cybersecurity risks, as traditional training methods do not track user performance effectively.

Objective

Commented [MR3]: @Mladinić,Roko R.

Our objective is to design and develop "PhishGuard", an interactive web-based simulation that gamifies cybersecurity training by challenging users to distinguish between safe and malicious e-mails that they receive. The aim of this project is to raise security awareness by creating as many different possible examples of malicious emails to educate users.

Points for the project

Commented [MR4]: @Mladinić,Roko R.

1. Interactive inbox (Frontend)
   This is the main screen that the user will interact with. It will resemble a real email client to make the simulation look realistic.

- Visuals: A list of incoming messages with subjects, senders, timestamps, and messages.
- Interactivity: Functional buttons that determine the user’s choice on whether the message received is safe or not.
- Timer: A countdown timer to increase pressure.

2. Content Library (Scenarios)

   This will be the “heart” of the project. It will contain the database for emails that the user will have to judge. It will contain both safe and malicious emails.

   - Phishing examples: Emails that contain malicious content will have a discrepancy, for example urgent requests for passwords, or fake lottery wins.
   - Safe Examples: Normal meeting invites, newsletters, or internal memos.
   - Difficulty Scaling: Level 1 is obvious spam; Level 3 helps users spot sophisticated "Spear Phishing" (targeted attacks).
   -

3. **The Immediate Feedback Loop (Education)**

   The project isn't just a test; it's a *teacher*. The user must learn instantly when they make a mistake.

   Correct Action: A positive sound effect and score increase.

   Incorrect Action: An educational "modal" (pop-up window) that pauses the game and explains the error (e.g., *"You clicked a malicious link! Notice how the sender's address was misspelled?"*).

Main Question

Commented [MR5]: @Mladinić,Roko R.

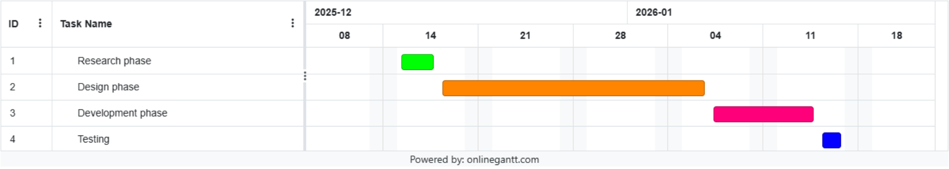
- How can we develop an interactive web-based simulation that effectively trains users to identify and reject phishing attacks in a realistic, risk-free environment?
- What technical features are required to create a simulated email interface that accurately mimics real-world working conditions and social engineering threats?

- What is the most effective way to provide immediate, educational feedback to a user the moment they fail to identify a security threat?

Planning

Commented [MS6]: @Markov,Simeon S.

For the planning phase, Trello was used (Agile methodology). For the gannt chart an online tool was used.



ID	Task Name
1	Research phase
2	Design phase
3	Development phase
4	Testing

Powered by: onlinegantt.com

Breakdown

- Week 1: Research and choosing a topic
  - During this week we spent our time thinking about what we wanted to do for our 2nd group project. We thought about the topics that related to what we've chosen for the 2nd semester and tried to come up with a passion project that would fit most of our interests.
- Week 2: Planning and Analysis
  - During this week we'll spend our time planning what the project we came up with will need to function properly. We'll think about things like our target audience and our project's requirements.
- Week 3: Design
  - During this week we'll spend our time designing the front-end and back-end of our project. We'll create a design for our database and think about what we want our website to look like. We'll work on writing the design document, planning the system architecture, and creating wireframes for the main components
- Week 4: Realisation
  - During this week we'll be creating our product. We'll spend our time by taking the ideas we got during the research, planning, analysis & design and turn them into a fully functional end-product.
- Week 5: Validation & Verification
  - During this week we'll spend our time testing our product. This week is meant for us to see if the features we created are working as intended. We'll also think

about what we could improve on.

Conclusion

This project plan is the foundation of our PhishGuard project. In this file we have mentioned the problem we want to solve, our objectives/goal and our planned approach. By focusing on an interactive and gamified solution, the project aims to improve cybersecurity awareness in a way that is more engaging than usual training methods. With this plan, the project is well prepared to move forward in an organized way.

Commented [MK7]: @Mizher,Kristiano K.G.