**Lab 2 – Phisecure Product Specification**

Hunter Pollock

Old Dominion University

CS411W

Professor Hosni

November 22, 2024

Version 2

**Table of Contents**

1. Introduction ……3
   1. Purpose ........3
   2. Scope of Project ........4
   3. Glossary ........4
   4. References ........5
   5. Overview of Document ....…7
2. Overall Description ……7
   1. Product Perspective ……7
   2. Product Functions ........8
   3. User Characteristics ........9
   4. Constraints ........9
   5. Assumptions and Dependencies ........9
3. Requirements ......10
   1. Functional Requirements ......10
   2. Non-Functional Requirements` ......12
   3. Performance Requirements ......13
   4. Assumptions and Design Constraints ......13

**List of Figures**

Figure 1- Phisecure Major Functional Component Design ........7

**List of Tables**

Table 1 – Phisecure RWP vs. Prototype Table ........8

1. **Introduction**

Phishing is a type of scam where attackers solicit information from victims masquerading as a legitimate person or business (NIST, 2024). They may ask for your password, or other financial details you typically wouldn’t share. Phishing is a serious and growing problem in the modern age. Over 3.4 billion phishing emails are sent daily, accounting for 1.2% of all email traffic globally. Additionally, 316,200,000 of those emails are targeted at one of the most vulnerable institutions: educational entities (Smith, 2024). Despite current attempts to tackle this problem, they still run into numerous issues that hinders the learning experience. Lack of hands-on experience, inadequate technology infrastructure, and resource constraints all play a part in the problem educational institutions have in training students and staff in this market. They need a new, innovative solution to phishing education.

Phisecure is designed to help alleviate these problems by providing an innovative and easily implementable phishing education environment to train its users. By providing a robust and up-to-date environment with knowledge on the latest and most current phishing information, we provide a service unlike others on the market that can greatly improve phishing education.

**1.1 Purpose**

The purpose of this document is to present a detailed overview of the Phisecure system This document is intended for the individuals of Team Orange and the teachers and staff at ODU to document and better display our work on Phisecure. It contains details on system specifications, user characteristics, the usage of the product, and its many characteristics.

**1.2 Scope of Project**

This product will be a web-based service for universities to utilize. We will offer up-to-date and interactive phishing training that can help train students more effectively than other solutions on the market. Instead of simply teaching students phishing education, we involve them in fake phishing attacks to demonstrate how phishing works and how to recognize attack attempts. By doing this, we maximize user retention and enjoyment in the process of learning and teach them on all the most up-to-date ways phishers try and scam them, preparing them for digital security challenges in the workplace.

**1.3 Glossary**

**Phishing** - The fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

**Spear Phishing** - A type of phishing involving personalization and targeting a specific individual.

**Malware** - Software that compromises the operation of a system by performing an unauthorized function or process.

**Ransomware** - A malware designed to deny a user or organization access to files on their computer.

**Attack** - An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

**1.4 References**

Irwin, L. (2023, June 19). *51 must-know phishing statistics for 2023: It governance*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023

Baker, E. (2024, January 23). *Top 10 costs of phishing - hoxhunt*. HoxHunt. http://www.hoxhunt.com/blog/what-are-the-top-10-costs-of-phishing#:~:text=Using%20different%20criteria%2C%20the%20Ponemon,as%20the%20king%20of%20cybercrime.

Stansfield, T. (2023, November 15). *Q3 2023 phishing and malware report*. Vadesecure. http://www.vadesecure.com/en/blog/q3-2023-phishing-malware-report#:~:text=in%20Q3%202023%2C%20Vade%20detected,180.4%20million

Toor, J. (2021, November 2). *Victims penetrated by phishing had conducted anti-phishing training*. Cloudian. https://cloudian.com/press/cloudian-ransomware-survey-finds-65-percent-of-victims-penetrated-by-phishing-had-conducted-anti-phishing-training/

Rezabek, J. (2024, January 24). *How much does phishing cost businesses?*. IRONSCALES. https://ironscales.com/blog/how-much-does-phishing-cost-businesses

Sheng, E. (2023, August 15). *Phishing scams targeting small business on social media including Meta are a “gold mine” for criminals*. CNBC. https://www.cnbc.com/2023/08/15/gold-mine-phishing-scams-rob-main-street-on-social-media-like-meta.html

Steves, M., Greene, K., & Theofanos, M. (2020, September 14). *Categorizing human phishing difficulty: A phish scale*. OUP Academic. https://academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453

Paun, G. (2024, February 20). *Council post: Building a brand: Why a strong Digital Presence Matters*. Forbes. https://www.forbes.com/sites/forbesagencycouncil/2020/07/02/building-a-brand-why-a-strong-digital-presence-matters/

Smith, G. (2024, February 16). *Top phishing statistics for 2024: Latest figures and trends*. StationX. https://www.stationx.net/phishing-statistics/

Alonso, J. (2023, July 18). *Universities warn of increased cyberscams targeting students*. Inside Higher Ed | Higher Education News, Events and Jobs. https://www.insidehighered.com/news/students/safety/2023/07/18/universities-warn-increased-cyberscams-targeting-students

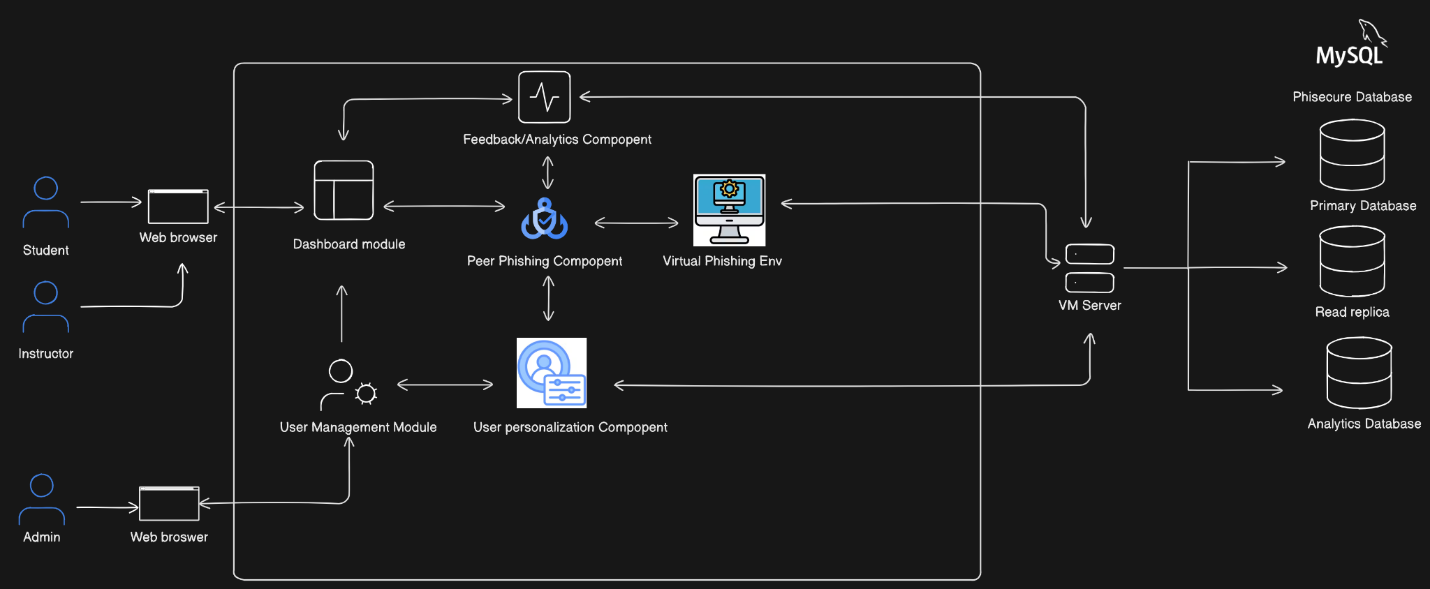
Cisco. (2024, February 22). *What is cybersecurity?*. Cisco. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

**1.5 Overview of Document**

The remaining sections of this document provide a general description of Phisecure. This includes hardware and software specifications, functional and data requirements, characteristics of Phisecure, and its users. Details on Phisecure are in sections 2.1 and 2.2. User characteristics are discussed in section 2.3. Other information and requirements are specified in Section 3

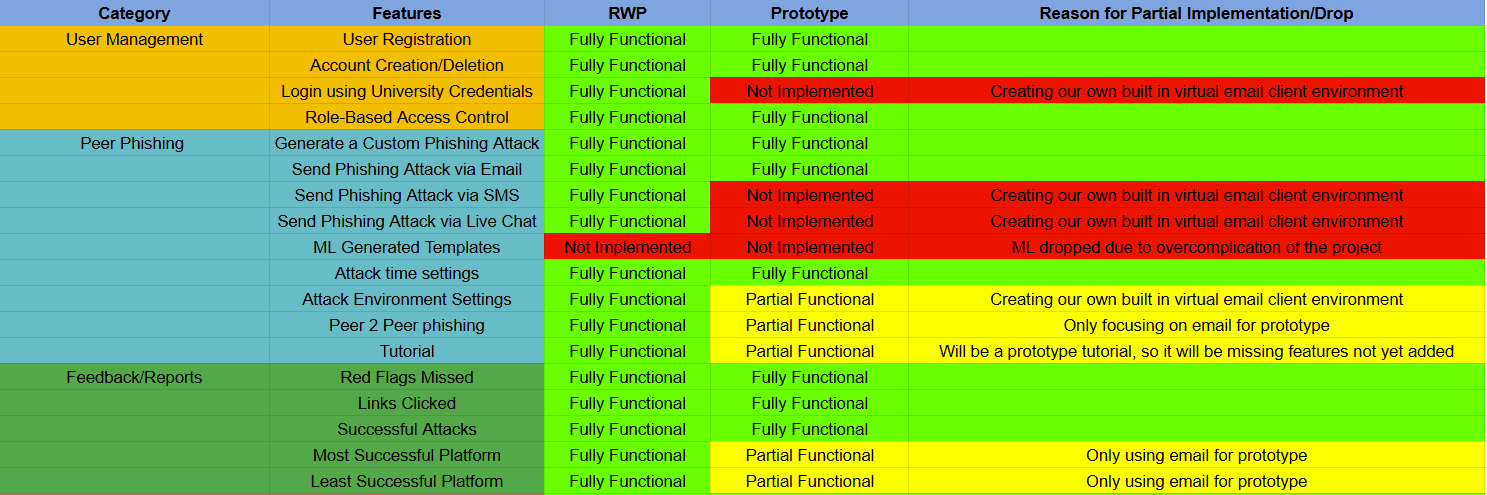
**2 Overall Description**

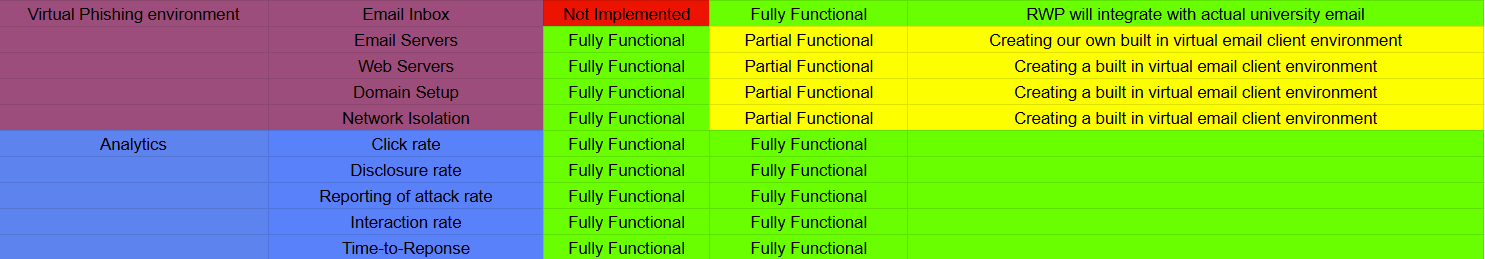
**2.1 Product Perspective**



Phisecure is a browser-based phishing education tool for universities. The intent is to provide an educational and interactive learning experience than other phishing training courses on the market that can more effectively train any student of it in the realm of phishing and how to avoid phishing attacks through methods like Peer Phishing.. We cover platforms like SMS, Zoom, Discord, and many other third-party messaging applications to provide a comprehensive solution. We can be incorporated into any cybersecurity class with how we’re designed for scalability for any class size.

**2.2 Product Functions**





One of the key features for Phisecure is Peer Phishing where users can send phishing attacks to peers and vice versa. Through this, users become more aware of what makes a competent phishing attack and the red flags that phishing attacks entail helping them to better recognize and avoid phishing attacks in the future. We also provide feedback and reports for users, that they may better understand the reasoning and logic behind the phishing attacks they encountered. With this, they gain a better understanding of their successes and failures and learn from them. Our virtual phishing environment that will be the basis of these attacks, from which we launch attacks and store data on them for future analysis. Finally, we have our analytics. These will show the details of attacks. How difficult or easy was it to fall for the attack? How long did it take to click on it? With this information, we can modify our templates and algorithms to better teach users the ins and outs of phishing.

**2.3 User Characteristics**

First up, we have **students**. These are the individuals who are using Phisecure to learn and are taking classes with it in the curriculum. They will perform phishing attacks against peers in their class, be phished themselves, and learn more about phishing through these attacks. Next up are the **admins**. These are the administrators of the Phisecure service, responsible for keeping everything running in top shape 24/7. They manage user information and signup, role and permission assignment, and analytics from both phishing attacks and overall system performance. **Instructors** are responsible for teaching their class(es) in Phisecure. They manage a class of students and their data. They also grab data from phishing attacks performed on their students through Phisecure to see how effective they were and if the students responded to it. Finally, we have testers. This is a development role for the creators of Phisecure that involves being able to assess and modify all aspects of the Phisecure system for release. That includes creating and managing students accounts (including the ability to create and delete them), creating simulations against oneself, sending feedback, validating user interface elements, and performing testing for all modules making up the Phisecure environment.

**2.4 Constraints**

N/A

**2.5 Assumptions and Dependencies**

N/A