Lab 2 - Phisecure Product Description

Ethan Barnes

Old Dominion University

CS411 Professional Workforce Development II

Professor Sarah Hosni

31 October 2024

Version 1

Table of Contents

[1 Introduction 3](#_7eysasxjyggk)

[1.1 Purpose 4](#_fw9twoinuzzs)

[1.2 Scope 4](#_25olgz3gr5cw)

[1.3 Definitions, Acronyms, and Abbreviations 4](#_sx2zjxgbg8qg)

[1.4 References 5](#_fhrbelfpsr04)

[1.5 Overview 8](#_ephcx8xgefh8)

[2 General Description 8](#_4bg191vow14k)

[2.1 Prototype Architecture Description 8](#_7sxxfihg59ht)

[2.2 Prototype Functional Description 9](#_pa9y3byhs3tn)

[2.3 External Interfaces 10](#_gzwcoccsx2sv)

[2.3.1 Hardware Interfaces 10](#_67826necyye7)

[2.3.2 Software Interfaces 11](#_4ema35e7sqym)

[2.3.3 User Interfaces 11](#_hk6uevadqh3p)

[2.3.4 Communications Protocols and Interfaces 11](#_dou8q4szc697)

List of Figures

Key Product Features and Capabilities……………………………………………………………………5

Major Components (Hardware/Software)....................................................................................................6

# 1 Introduction

Phishing attacks are becoming more frequent and more sophisticated. A significant rise in phishing attacks occurred during Covid with an increase of 220% compared to pre-Covid years (David, 2019). Though these attacks have not returned to their previous Covid peak, they are still increasing year after year.

With the rise of phishing attacks there has also been a rise in products on the market. From paid to open-source, there is a plethora of systems to choose from. However, many of these are falling short as evidenced by the rise in successful phishing attacks (Desi, 2024).

Phishing attacks are also more complicated than ever. Spoofed links are using HTTPS certificates, and all end destinations for stolen data use TLS encryption (David, 2019). The majority of attacks are also using popular name-brand logos and headers, imitating companies like Amazon, Apple, and Netflix. The most targeted sector for phishing is Education (David, 2019). There is a gap in phishing education targeted towards Universities, and that is where Phisecure enters.

Universities seeking to provide the best education need to establish better phishing education, especially with a focus on real-world scenarios. Phisecure aims to be the tool Universities will use to educate their students about preventing phishing attacks.

## 1.1 Purpose

This SRS is intended for developers to understand Phisecure on a technical level. The document will go into detail about the interfaces and functions that will be available in the prototype. The intended audience is academic staff, including Teacher Assistants, Graduate Students, or Professors.

## 1.2 Scope

Phisecure has the tools that minimizes the threat of phishing attacks.. Using a controlled environment, a user can be exposed to any new techniques developed by nefarious parties. Phisecure will create templates based on simulated target information. Reports on whether the target successfully defended an attack or not are generated for authorized users. A unique feature is the use of custom templates for collaborative phishing simulations among your fellow users.

Whether it is used for phishing education for new students or a more in-depth dive into Cybersecurity, Phisecure has the flexibility to be the best tool for Universities. All the attacks will take place in a controlled environment where there is no risk of an attack occurring. Users with Admin and Instructor/Researcher access will have complete control over what Student users can do, as well as access to valuable feedback and reports.

## 1.3 Definitions, Acronyms, and Abbreviations

**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

**SRS -** Software Requirements Specification

**SMS** - Short Messaging System

**VoIP** - Voice over Internet Protocol

**POP** - Post Office Protocol

**SMTP** - Simple Mail Transfer Protocol

**HTTP** - Hypertext Transfer Protocol

**IMAP -** Internet Message Access Protocol

## 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-penet rated-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-m edia-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-str ong-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-increa sed-cyberscams-targeting-students

Cisco. (2024, February 22). *What is cybersecurity?*. Cisco.

https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

David Warburton, R. P. (2019, October 24). *2019 phishing and fraud report*. F5 Labs. https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud-report#:~:tex t=In%20the%20F5%20Labs%202019,breach%20reported%20by%20U.S.%20companies. &text=Because%20phishing%20can%20commonly%20grant,of%20some%20of%20these %20breaches.

Desai, D., Hegde, R., Laufer, E., & Wang, J. (2024, April 9). *2023 phishing report reveals 47.2% surge in phishing attacks last year*. Zscaler.

https://www.zscaler.com/blogs/security-research/2023-phishing-report-reveals-47-2-surge phishing-attacks-last-year

## 1.5 Overview

The remainder of this document will provide descriptions for the architecture and functional design. Additionally, the external interfaces will be described.

# 2 General Description

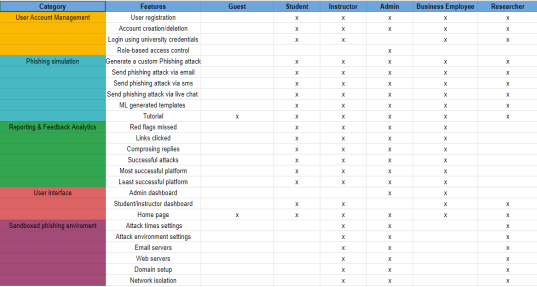
Phisecure is a web application with multiple user roles. Each role will have its own respective dashboard. The prototype will demonstrate email phishing attacks, while other types that would be in the real world product support SMS and VoIP.

## 2.1 Prototype Architecture Description

A Student user will first create an account. They will provide what communication systems they use and the affiliated usernames for said accounts. Depending on whether they’ve been granted access for peer-to-peer phishing, they may conduct phishing attacks on other Student users or they can have their instructor launch a phishing attack campaign on them. They will also receive reports regarding how successful their peer phishing attacks were as well as how adequate they were defended against phishing attacks.

An Instructor user will also have to create an account. They have access to all features that a Student user has. In addition, they can also create Phishing Attack Campaigns. In these Campaigns they will be able to choose the time and type, but Phisecure will handle the rest as far as what template to select. The reports available are not just individual reports, but whole course sections if the Instructor user chooses.

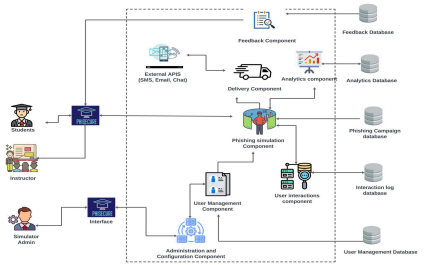
The Admin user has access to all previously mentioned features, but they also can revoke, modify, or grant access to users. In the future, Business Employees and Researchers can make use of Phisecure in their respective settings and have features similar to a Student user and Instructor, respectively.



## 2.2 Prototype Functional Description

The frontend will be created with the React framework, using Python, HTML, and CSS in VS Code. The interfaces will be what all users see and access for Phisecure. Once a user creates a phishing attack, whether peer phishing or a campaign, their data will be sent to the backend. The backend will be running on the Flask framework and be written in Python on VS Code. The backend will pull data from MySQL and Amazon RDS databases to find appropriate phishing templates, as well as pulling Student user feedback, Instructor user reports, and other analytics used to create more effective reports and attacks.

Third-party APIs include Twilio, MailGun, and Live Chat. Twilio is for SMS phishing, MailGun for email, and Live Chat for the suite of video messaging services.



## 2.3 External Interfaces

As a web application Phisecure aims to be accessible through all major desktop browsers.

### 2.3.1 Hardware Interfaces

Hardware includes any machine capable of running a desktop browser.

### 2.3.2 Software Interfaces

The prototype requires the Docker Platform, React Framework, Flask Framework, and MySQL

### 2.3.3 User Interfaces

Internet access, mouse, and keyboard are essential for operation.

### 2.3.4 Communications Protocols and Interfaces

The system is web-based and uses HTTP protocols. The inclusion of Email requires SMTP, IMAP, POP protocols.