Lab 2 - Phisecure Product Description

Hunter Pollock, Ralph Mpanu-Mpanu, Dylan Via, Joshua Freeman, Ethan Barnes, Mustafa Ibrahim

Old Dominion University

CS411W Professional Workforce Development I

Professor Sarah Hosni

22 November 2024

Version 2

Table of Contents

List of figures

1. Introduction

Phishing is a significant cybersecurity threat that targets millions of individuals worldwide. Phishing is a form of criminal social engineering that is conducted through digital communication channels such as email, voice calls, websites, or text messages. In today's digital age, universities are prime targets for phishing-related attacks (David, 2019). Phishing makes up about half of cyberattacks against higher education (Oxman, 2023). In 2022, Duke University experienced a phishing campaign which attacked students and tried to bait them into sharing login information with the threat of losing account access (Oxman, 2023).

It is clearly imperative that universities must take phishing threats seriously or face consequences such as financial losses, reputation damage, and data breaches. Due to the social engineering nature phishing, human error remains one of the primary reasons victims fall prey to these attacks. Social engineering can be defined as a scam where the criminal impersonates someone else, a group, or a brand to manipulate the victim to perform a certain action (Oles, 2023). The most serious cyber threats such as ransomware and malware stem from phishing attacks due to the low cost and the ability to easily scale (Oles, 2023).

To combat these threats, universities must implement a comprehensive strategy that goes beyond traditional education methods. This should include interactive learning opportunities, allowing students and staff to gain hands-on experience in recognizing and responding to common phishing attacks.

1.1. Purpose

Phisecure is a web application that provides personalized phishing simulations tailored to the user. Phishing techniques used during the simulation will be reported and explained to the user upon completion. The goal is to provide students, faculty, and administrators with a secure learning environment that offers realistic phishing scenarios they might encounter in the real world. Users they learn best practices and recognize red flags in phishing scenarios.

1.2. Scope

The prototype will allow students to create and send phishing emails to their peers and track real-time interactions after every simulated phishing attempt. The simulation feature will select personalized templates that relate to the user. The goal of these phishing attempts is to elicit interaction from the user such as replying with personal information (this will be deleted), clicking a link or downloading an attachment, and lastly if the user detects the phishing attempt users can report the email.

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.

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

Oxman, Z. (2023, July 13). Protecting Higher Education from Email Attacks. Abnormal Security. Retrieved from https://abnormalsecurity.com/blog/protecting-higher-education email-attacks

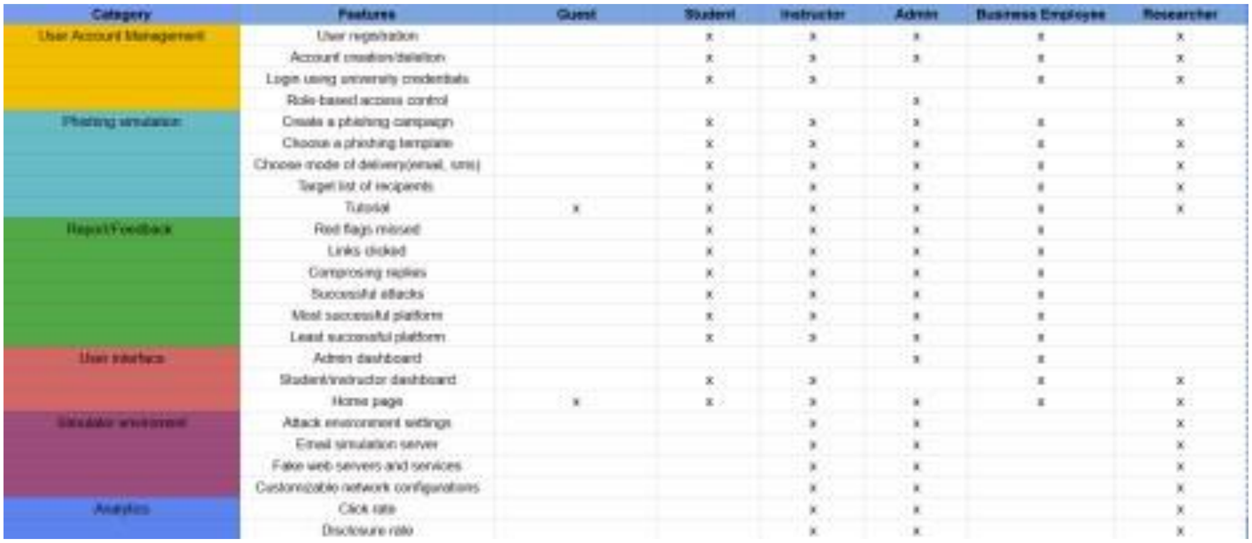
Oles, N. (2023). *How to Catch a Phish.*

2.1 Product Perspective

Phisecure is an educational software tool that simulates phishing attacks. It provides direct cybersecurity training in a controlled environment. Users can create customized phishing campaigns that simulate attacks across multiple digital platforms such as email, SMS, and live chat. Each campaign includes details like the name, description, launch date, end date, and status of the current campaign. Built as a web application the frontend use React framework with HTML, CSS, and JavaScript. The backend utilizes Flask framework using Python. Data is stored using Amazon RDS MySql.

2.2 Product Functions

Figure 1



Category	Features	Guest	Student	Instructor	Admin	Business Employee	Researcher
User Account Management	User registration		x	x	x	x	x
	Account creation/deletion		x	x	x	x	x
	Login using university credentials		x	x		x	x
	Role-based access control				x		
Phishing simulation	Create a phishing campaign		x	x	x	x	x
	Choose a phishing template		x	x	x	x	x
	Choose mode of delivery(email, sms)		x	x	x	x	x
	Target list of recipients		x	x	x	x	x
	Tutorial	x	x	x	x	x	x
Report/Feedback	Red flags missed		x	x	x	x	
	Links clicked		x	x	x	x	
	Comprosing replies		x	x	x	x	
	Successful attacks		x	x	x	x	
	Most successful platform		x	x	x	x	
	Least successful platform		x	x	x	x	
User interface	Admin dashboard				x	x	
	Student/instructor dashboard		x	x		x	x
	Home page	x	x	x	x	x	x
Simulator environment	Attack environment settings			x	x		x
	Email simulation server			x	x		x
	Fake web servers and services			x	x		x
	Customizable network configurations			x	x		x
Analytics	Click rate			x	x		x
	Disclosure rate			x	x		x

The features in Phisecure can be broken down into several categories. User management, phishing simulation, reporting/feedback, user interface, simulator environment, and analytics. The core features in the product are the phishing simulation, reports/feedback, and analytics. The phishing simulation facilitates the creation of the phishing campaigns, including the selection of templates and modes of delivery.

The system collects data from users interacting with the campaigns to make sure they following best practices if they give up sensitive information or compromising data. This data will be primarily collected via interaction log. Once the simulation is complete, feedback will be assessed. Feedback includes red flags missed, links clicked, compromising replies, and most/least successful platforms. Feedback is used to generate performance reports for student users and allow instructors to assess their students. This interaction data generates insightful analytics such as click rate, disclosure rate, and interaction rate.

2.3 External Interfaces

Phisecure will utilize various hardware, software, and interfaces to provide comprehensive cybersecurity training platform.

2.3.1 Hardware Interfaces

The application requires a PC with internet access, supporting operating systems such as Windows.

2.3.2 Software Interfaces

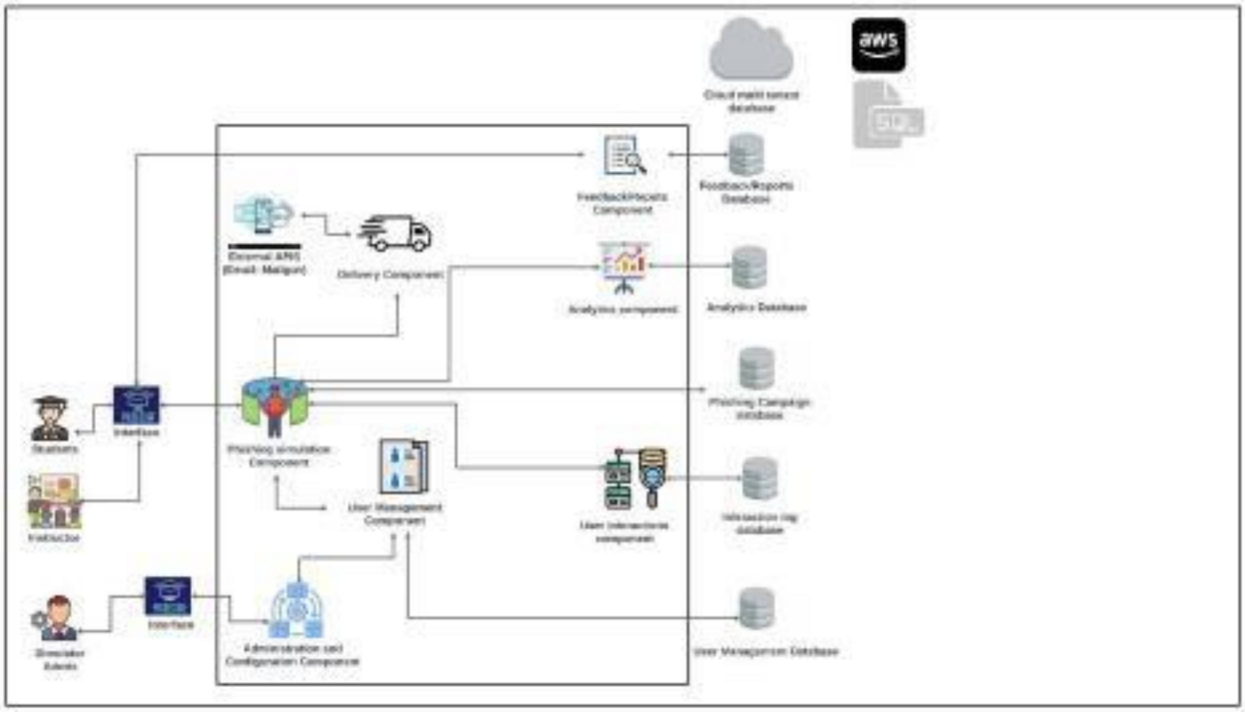
Software will include the application's frontend built, with React and backend using Flask. It also includes a virtual environment hosted by AWS. For data storage Amazon RDS MySQL will be used. In addition, external APIS, such as Twilio, Mailgun, and Live Chat APIS deliver simulated phishing attacks across multiple platforms.

2.3.3 User Interfaces

Phisecure is accessible via a web application which requires a desktop with internet access. Users will primarily interact with the web app through a standard web browser such as Google chrome, Firefox, Microsoft Edge.

Figure 2

Major Functional Component Design


Cloud multi tenant database
Feedback/Reports Component
Feedback/Reports Database
External APIS (Email: Mailgun)
Delivery Component
Analytics component
Analytics Database
Phishing Campaign database
Students
Interface
Phishing simulation Component
User Management Component
User interactions component
Interaction log database
Instructor
Simulator Admin
Interface
Administration and Configuration Component
User Management Database