Lab 1 - Phisecure Product Description

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

Old Dominion University

CS410 Professional Workforce Development I

Professor Janet Brunelle

27 April 2024

Version 1

Table of Contents

List of Figures

1. Introduction

Phishing has been a recurring problem since the dawn of communication technologies. It is evolving and growing in scale as the years go by. Educating users on this issue is a hard feat to accomplish due to the scalability of the issue. New methods are being introduced every day. Preparing people for future attacks by using outdated examples and generic policies/warnings to adhere to is not going to be effective enough.

Phishing has been a successful method for criminals to gain access to otherwise restricted areas. With a report of 91% of system breaches being caused by phishing attacks (Alkhalil, Hewage, Nawaf, & Khan, 2021). We can confirm that it is the most popular method used today. Educational efforts to train people and prepare them for phishing attacks have to go beyond a simple education of phishing and training in spotting attacks. A study was conducted doing exactly this and found no significant increase in phishing detection from the participants (Alghamdi, n.d.).

This issue can be a huge hit to businesses financially. From this report, the average cost of a data breach for a business on the global scale was $4.45 million in 2023 (Dergacheva & Taylor, 2024). This scare of a potential financial hit from phishing is a motivator for businesses to educate their employees on phishing attacks.

University students can be potential victims of phishing also. With recent reports being made about such events at California State University (Alonso, 2023). Students were warned that their Office 365 account was going to be terminated from dual account issues, unless they verified their account using the url provided to them within 24 hours.

The widespread cases of phishing and persistent success of the attacks create a demand for a solution. Universities offering an innovative course to expose their students to phishing attacks and train them on phishing detection has a place in today's world. So much more is done online than ever, so proper training to identify an imposter is needed.

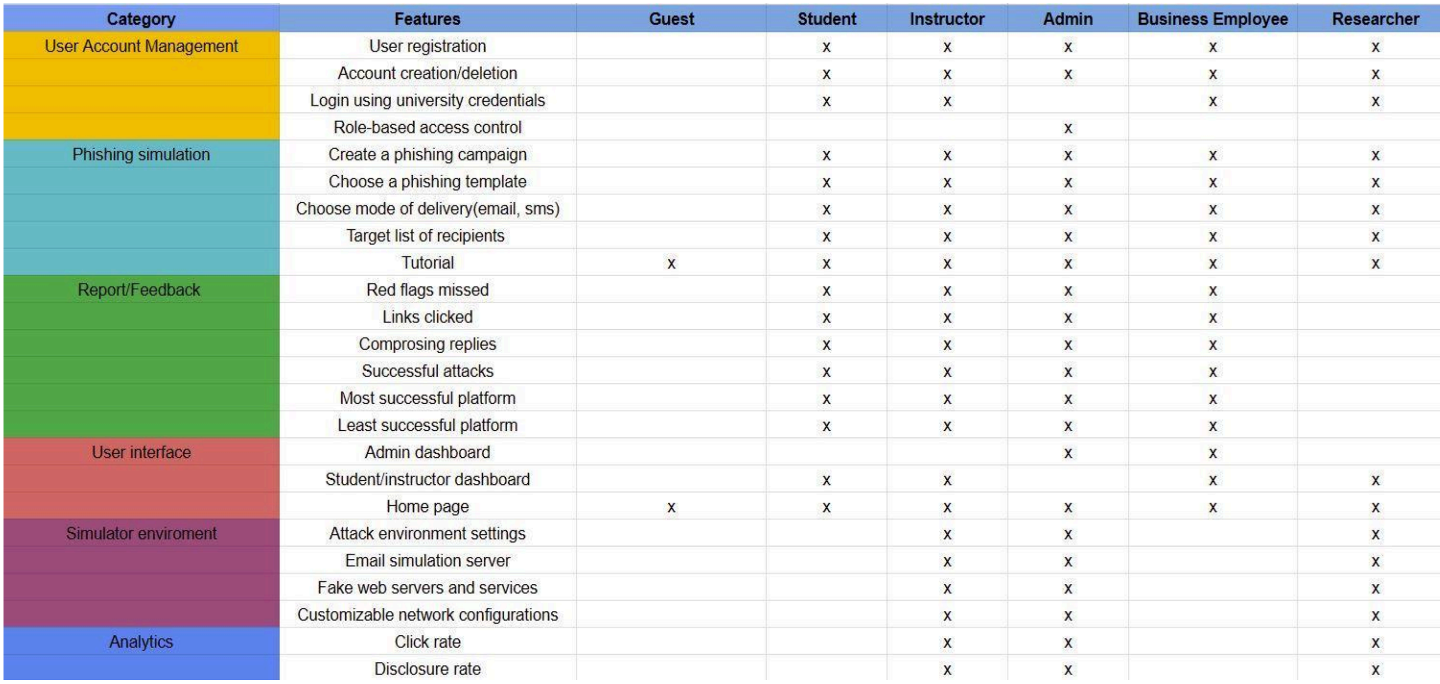
2. Product Description

Phisecure is a tool designed to create an innovative educational experience for phishing. Automatic generation of phishing messages to be used in simulated campaigns against the students. Then providing an in depth report on how the students performed and what methods were used against them. Instructors will be paired with the tool, receiving their own reports on how well the students performed, to create a well rounded educational experience. The goal is to provide first hand experience to the students by phishing them and showing how susceptible they are to these attacks and educating them on the detection of these types of attacks.

2.1. Key Product Features and Capabilities

Figure 1

Features Table



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 enviroment	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

To accomplish this goal Phisecure will receive inputs from the student to create tailor made phishing messages to be used in simulated campaigns. After the campaign is finished, students receive feedback and reports that discuss how well they performed and what red flags should have been detectable in the messages used on them.

The instructor will have the ability to review the performance of the students. They will have their own reports designed to provide data that can be used for educational purposes. They will also have privileges to design campaigns to provide a more effective learning experience.

The product will simulate more than just email phishing attacks. Phisecure will have the capability to send phishing attacks through a variety of methods. Email, phone, and third party chat API's that the user interacts with. This variation will promote safe practices with more than just email and allows students to experience what forms these attacks can take.

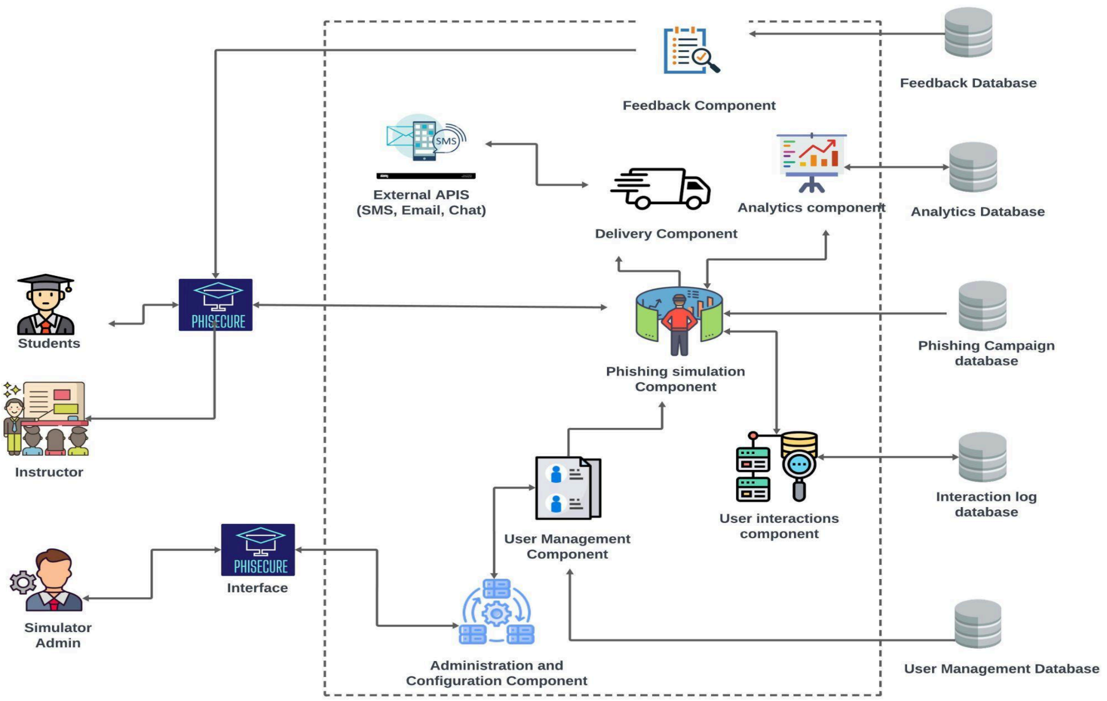
Peer Phishing is an innovative feature that will be added to Phisecure. This will allow students to play the attacker, choosing another student to attack. They will design their own template for the product to use and will be updated on how successful their attack was. Phisecure will save successful templates for review and possible storage, allowing the template database to grow with the help of the students interacting with Peer Phishing. Figure 1 showing an assortment of these features by category.

2.2. Major Components (Hardware/Software)

Phisecure will have a front end interface for users, backend for algorithms and database, and external services for needed functionalities. Figure 2 is the Major Functional Component Diagram for the Phisecure solution.

Figure 2

Major Functional Components Diagram



Front-End

Phisecure uses React as the front-end framework. Python, HTML, and CSS will be the coding languages used. The Integrated Development Environment used will be VS Code. The front-end user interfaces will be responsible for prompting users for important inputs needed for message creation and simulation. It will also be interacted with by users to output the reports and feedback.

Back-End Algorithms

On the server-side the project will employ Flask as the framework. The back-end will be primarily developed in Python language, leveraging Flask. The Integrated Development Environment used will be VS Code. The back-end will implement algorithms to match student information to templates and develop phishing attacks and send them to their selected environment path. It will also be responsible for retrieving interaction data from the messages sent to collect data and create reports.

Back-End Database

The database will use Amazon RDS and MySQL for database management. Amazon RDS allows easy setup, operation, and scaling of the relational database in the cloud. MySQL will be the specific engine to run within Amazon RDS. It will handle the actual storage, retrieval, management, and modification of the data.

Version Control

The version control system will be Git, to employ efficient handling of version history and collaboration. The Repository that will be used is GitHub. GitHub is an effective and reliable hosting service. It will provide tools necessary for team collaboration and code review.

External Software

MailGun API will be incorporated into the software to send email messages. Twilio API will be incorporated to handle SMS messaging. Variety of Live Chat API will be used by the software to send their respective messages.

3. Identification of Case Study

Our proposed case study involves Old Dominion University (ODU), located in Norfolk, Virginia. This university, having a strong focus on advancing cybersecurity education amidst increasing phishing incidents, represents an ideal setting for implementing Phisecure. The potential collaboration with ODU would allow us to tailor a unique course that leverages Phisecure, providing students with unrivaled hands-on experience in phishing detection and response.

4. 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.

5. 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

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, January 18). *Phishing attacks: A recent comprehensive study and a new anatomy*. Frontiers. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

Alghamdi, H. (n.d.). *Can phishing education enable users to recognize phishing attacks?*. ARROW@TU Dublin. https://arrow.tudublin.ie/scschcomdis/99/

Alonso, Johanna. "*Going Phishing on Campus*." Inside Higher Ed, Inside Higher Ed, 18 July 2023, www.insidehighered.com/news/students/safety/2023/07/18/universities-warn-increased-cyberscams-targeting-students

Dergacheva, A., & Taylor, J. R. (2024, March 6). *Study finds average cost of data breaches continued to rise in 2023*. Study Finds Average Cost of Data Breaches Continued to Rise in 2023 –. https://www.morganlewis.com/blogs/sourcingatmorganlewis/2024/03/study-finds-average-cost-of-data-breaches-continued-to-rise-in-2023