**Lab 1 - Phisecure Product Description**

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

Old Dominion University

CS410 Professional Workforce Development I

Professor Janet Brunelle

29 April 2024

Version 1

**Table of Contents**

[1. Introduction](#_Toc164227006)

[2. Product Description](#_Toc164227007)

[2.1. Key Product Features and Capabilities](#_Toc164227008)

[2.2. Major Components (Hardware/Software)](#_Toc164227009)

[3. Identification of Case Study](#_Toc164227010)

[4. Glossary](#_Toc164227011)

[5. References](#_Toc164227012)

**List of Figures**

Figure 1: Phisecure Features Table 4

Figure 2: Phisecure Major Functional Component Design

# Introduction

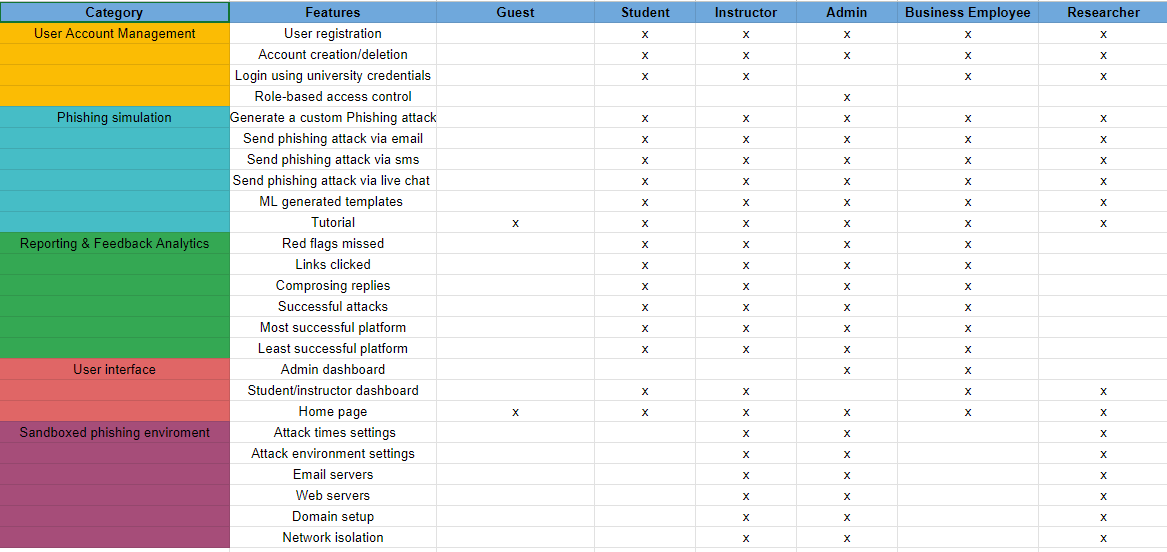
As things currently stand, Universities do not have quality, innovative tools to educate their students, faculty, and staff about the threat of phishing. Phishing is a scam where the perpetrator acquires sensitive data, such as bank account numbers, through a fraudulent solicitation in emails or on a web site masquerading as a legitimate business or reputable person (*phishing – Glossary*, 2024). This can also be done through other mediums, like SMS (“smshing”), and IM apps (Discord, Skype, etc.). And it’s a very serious problem. Over **316,200,000** phishing emails are sent to universities per *day*(Smith, 2024)! **27.8%** of educational facilities fall for phishing attacks across all spectrums including universities, making them some of the most vulnerable for phishing attacks(Smith, 2024). California State University (CSU) had **82** student accounts compromised in Q2 of 2023 (Alonso, 2023). Students were locked out of their accounts ,and the university had to spend time, money, and resources restoring the account from the phishing attack. **Lack of Hands-On Experience, Outdated Technology**, **Resource Constraints, Lack of Scalability** all contribute to this problem. **Phisecure** intends to help alleviate this problem by creating an innovative new tool to teach students, staff, and faculty at universities about phishing. With **Phisecure**, your students and staff will be much more likely to be aware of phishing and not bite the hook when the phishers come to dangle the hook with our innovative approach to our teaching tools and software. We can provide hands-on experience with phishing with technology up to date with modern standards. With our product, universities won’t have to struggle with resource constraints or lack of scalability either, as our product is both easy to implement and scale whether you’re teaching a class of five, or a class of thirty. With **Phisecure**, phishing training has never been easier or more engaging, nor so easy to implement.

# Product Description

## Key Product Features and Capabilities

**Figure 1**

*Features Table*



As you can see here, we want to make Phisecure more than just another Phishing educational tool. We want to make it educational and interactive, something all users will more actively interact with. Let’s start with one of our main selling points: **Peer-driven Spear Phishing**. You can send phishing attacks to your peers as well as be sent phishing attacks by both Phisecure and your other peers. Everyone is part of helping one another learn how to be more aware of phishing. And it’s not just for email, either. We include other avenues like SMS and third party applications like Zoom, Discord, Slack, and Microsoft Teams. While we’re not an all-encompassing product, we do want to offer more avenues to train your students in phishing that better reflect the diverse phishing landscape of the modern internet era. We’re free for universities: No money needed. It can be implemented into cybersecurity courses or made as the basis for one. The objective of Phisecure is simple: To provide a robust and interactive educational environment to teach phishing to users.

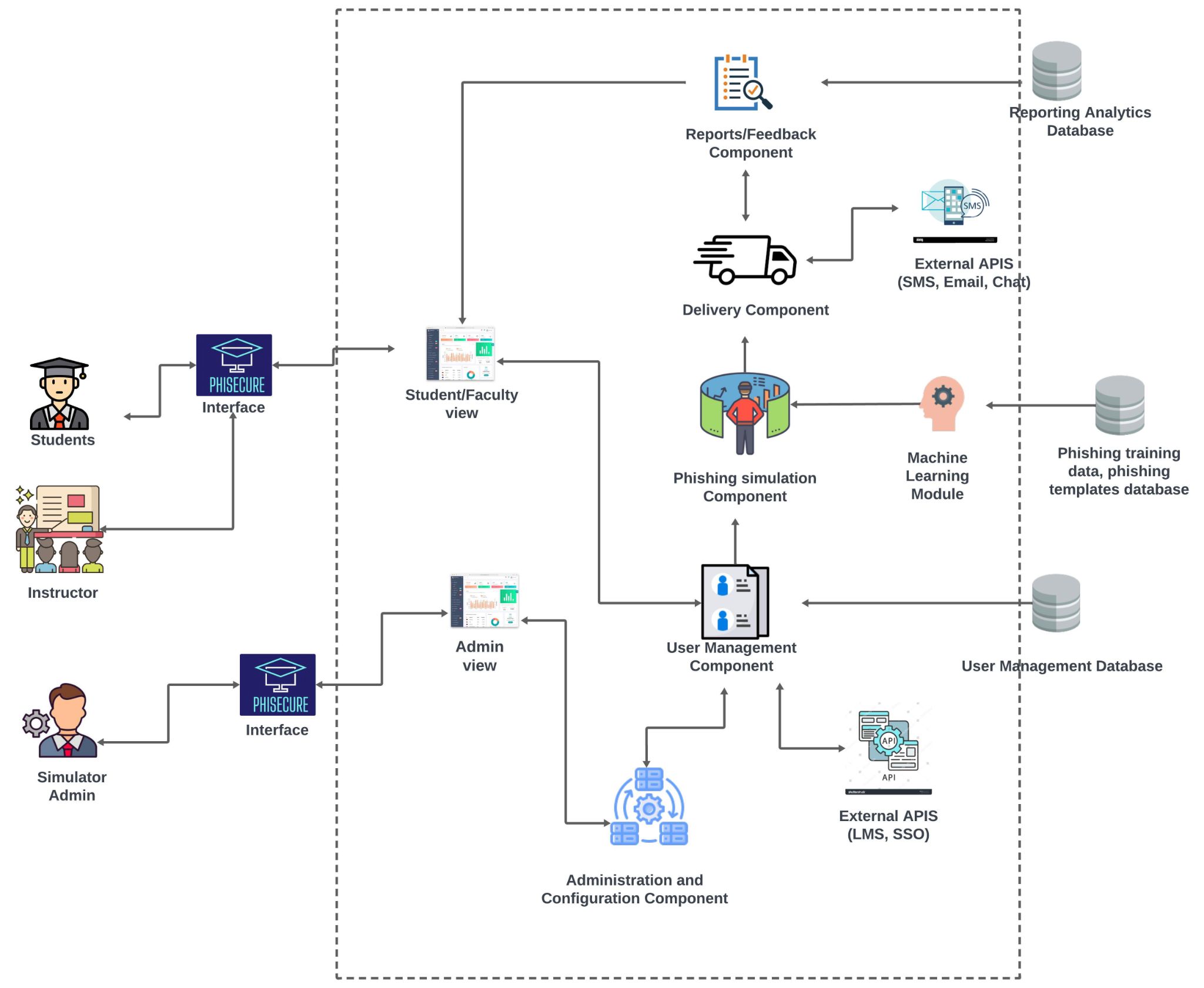
## Major Components (Hardware/Software)

Phisecure is intended to be a cross-platform web application/service. The front end

portion will use React JavaScript library as a framework, alongside including the languages Python, HTML, and CSS. The back end will use the Flask Python framework and include the Python language. Both the front and back ends will use VSCode for the IDE. Both will interact with databases hosted by Amazon Web Services (AWS) with structured query languages (SQL). We will also be implementing various third party APIs for message through their respective services (Discord, Slack, etc).

**Figure 2**

*Major Functional Component Design*



# Identification of Case Study

Phisecure is originally made with the premise to be of use to universities to assist in training their students, staff, and faculty. Whether by use it as a basis for a course in phishing security or added on top of an existing Cybersecurity course. It’s a new and innovative solution to phishing education that goes a step above the existing products and solutions out on the market. With our feedback and analytic tools, teachers have an easy way to check where their students may be struggling in terms of phishing recognition. But our product’s benefactors don’t just start and stop at universities. Local businesses around universities implementing Phisecure can also benefit from this tool. After all, it’s a very growing problem in the modern age, and as stated before in section 1, businesses rely more and more on an internet presence to grow, leaving them vulnerable to phishing attacks. Phisecure helps in two ways. Firstly, it helps IT students grow their knowledge pool on phishing before heading into the workforce with their degree, an asset that not only helps them secure jobs, but also provides value to the businesses. Less time needed to train those students in phishing and helps them better call attention to potential scams that the company might come across. Secondly, it provides an easy solution to phishing training. Simply send employees over to the university to take courses with Phisecure in them. They’ll come out more knowledgeable and better prepared for phishing than ever before.

# 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.

# 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