



# PHISECURE

PHISHING EDUCATION: TO BE  
AWARE, DON'T BITE THAT HOOK

## CS410 Feasibility Presentation

By: Team Orange (2024)

3/15/24

# Table of Contents

3-5. Team Member

6-16. The Problem

17-21. The Solution

22. Major Functional Component Design

23-25. Phisecure: Its uses and its Users

26. Competition Comparison

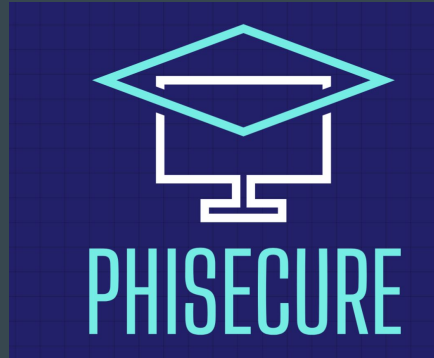
27-29. Risk Matrix

30. Conclusion

# Team Members



Hunter Pollock is a Senior at ODU currently studying and majoring in Computer Science, with the goal of getting a Master's degree in the graduate program. He enjoys playing video games, good food, listening to music, and learning about programming.



Ethan Barnes is another Senior at ODU, studying Computer Science. He is currently working at a flour mill as a Second Miller. He enjoys reading, the outdoors, and discovering new things. He has three children.

# Team Members



Joshua Freeman is a senior at ODU and is majoring in Computer Science. He like to read and play video games.



Dylan Via is an undergraduate student at ODU going for his bachelors in Computer Science. He plans on pursuing a career in Software Engineering after he graduates. Most of his training in coding has been in C++, but he does have experience in Java and Python.



Ralph Mpanu is a senior at ODU and is majoring in Computer Science. After graduating he plans on working as a software engineer. He enjoys fitness and practicing brazilian jiu-jitsu.

# Mentor

Mustafa Ibrahim is a PhD student at ODU, specializing in Computer Science with a focus on Cybersecurity, particularly in Networking Security. He also enjoys playing soccer.



# Field of Cyber Security

- Cybersecurity is a field/practice that involves protecting systems, networks, and programs from digital attacks.<sup>18</sup>
  - This involves various practices like proper digital education, programs, and systems that prevent digital attacks from going through
- Why is it important?
  - “At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like family photos. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.”<sup>18</sup>

# Cyber Security Education

- Educational institutions especially know the importance of proper cybersecurity practices and education. They are responsible for protecting their staff, faculty, and students from vulnerabilities.
- Yet, the threat of cybersecurity keeps rising for educational institutions.
- For example, here's one story from a university of a particularly big phishing scam...

# Universities - Some Background...

- Students were getting emails about their Office 365 accounts being terminated if they didn't cancel the request
- Except they *weren't* being terminated to begin with. It was a scam by a phisher to grab student info and hack into other student emails to extort them for money.<sup>17</sup>
- Stories such as this are occurring more frequently throughout the world at universities. Phishers are always changing tactics and getting smarter in how to perpetrate these crimes.
- This proves to be a massive challenge for universities. Why?



# Problem Statement

Universities need innovative educational tools for teaching cybersecurity to their faculty, staff, and students so they can better identify and avoid phishing attacks.



# Phishing

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<sup>13</sup>. This can also be done through other mediums, like SMS (“smshing”), and IM apps (Discord, Skype, etc.). This is done through vulnerabilities: weaknesses that phishers exploit. These can be things like weaknesses in the infrastructure of the tech, or lack of awareness on the part of the users.



# Threat - Phishing

- Phishing is becoming more and more common in the modern world
  - Over **3.4 billion** phishing emails are sent a day, and email phishing accounts for **1.2%** of all email traffic globally!<sup>16</sup>
  - **84%** of organizations [of all kinds] were the target of at least one phishing attack.
  - Education industries (such as universities) make up **9.3%** of these attacks.
    - That might not sound like much at first, but that's **316,200,000 emails per DAY** targeted at educational institutions!

# Mo' Phishing, Mo' Problems




# Mo' Phishing, Mo' Problems

Universities, as stated before, are some of the most vulnerable institutions in terms of phishing attacks. California State University would know.

- **82** student accounts of theirs were compromised in Q2 of 2023, up from almost zero at the beginning of 2021.<sup>[17](#)</sup>
- These attacks pose as either threatening to shut down access to important services like email accounts or offering students jobs with very enticing pay.
  - The second one especially is tempting, as many newer students need the money to support themselves, especially those who moved to live near the university (especially those from out of town and/or state).
- Don't think it's just them either: The scam is present throughout most universities, as it's very tempting for newer students and others who might not be as aware of the tells of phishing scams. For example...

# Mo' Phishing, Mo' Problems

Phishing scam "Downsizing Musical Instruments and Items" Inbox x 🖨️ 🔗

 **ITS Help** <itshelp@odu.edu>  
to ▾ Thu, Mar 7 10:31AM (12 days ago) ★ ↶ ⋮

Dear ODU Community,

ODU users have been targeted by Musical Instruments phish. The scam emails were sent as opportunity to buy reduced cost musical instruments with the subject line: ***"DOWNSIZING MUSICAL INSTRUMENTS AND ITEMS."***

This is not a legitimate email. If you received one of these messages:

1. Do not engage with the soliciting party.
2. Do not supply any personal information (name, address, social, banking/credit card).
3. If you've already started a conversation, stop any further contact.
4. If you forwarded the scam email to anyone, please pass this notice along as well.
5. If you responded to the job scam email, provided personal information, and are concerned about your identity, contact the ODU Police at [police@odu.edu](mailto:police@odu.edu).

We've seen an increase in phishing attacks and DUO "prompt bombing" lately. To combat these types of attacks, we must all remain aware and vigilant.

For more information on cybersecurity, please visit our awareness page at [www.odu.edu/safecomputing](http://www.odu.edu/safecomputing)

Thank you for your diligence in maintaining a secure ODU computing environment.

Kate Rhodes  
Interim CISO | Information Technology Services  
Old Dominion University  
Phone: (757)683-5404  
Email: [kprhodes@odu.edu](mailto:kprhodes@odu.edu)  
[Computing Security - Old Dominion University \(odu.edu\)](http://www.odu.edu/computingsecurity)

# Phishing Education

It's becoming more and more clear students and faculties at these universities do not have the proper training required to discern phishing scams from legitimate emails

- The average click rate for a phishing attack is **17.8%**, going to to **53.2%** for more targeted spear phishing attacks!<sup>16</sup>
- As well as all this, educational facilities have been reported to be some of the most likely to fall for phishing attacks, opening the emails **27.8%** of the time! It's becoming more and more of an issue, and educational institutions like universities are some of the most vulnerable entities out there.

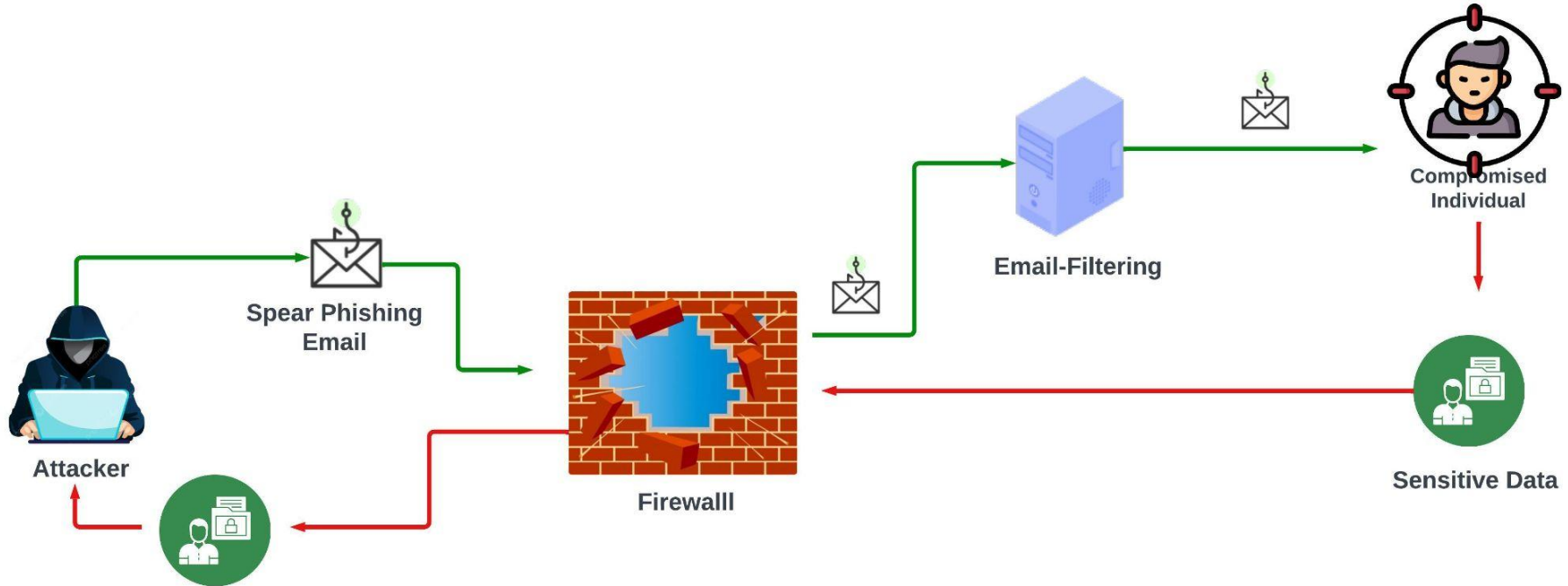
**Universities need a proper way to train their students so that they don't bite the hook.**

# Problem Characteristics

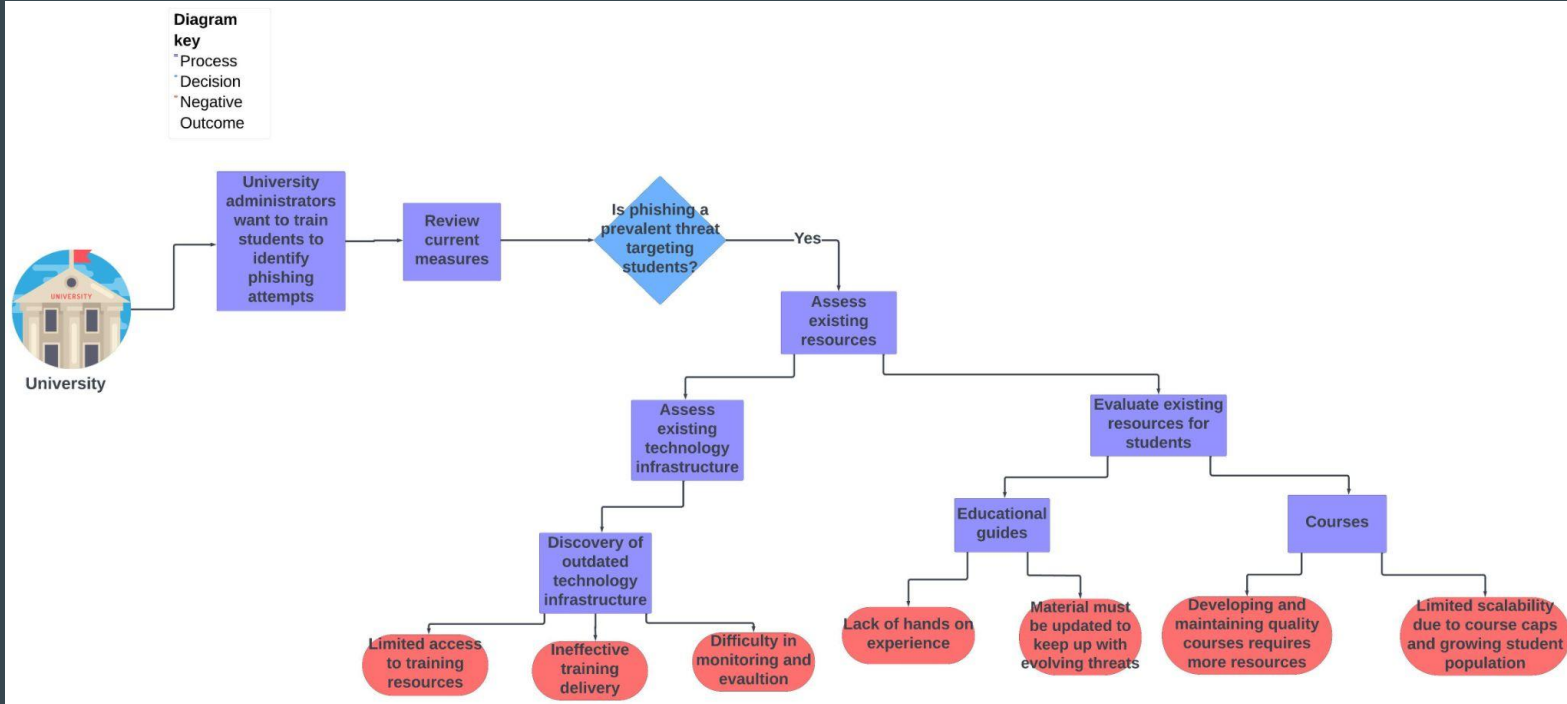
- **Lack of Hands-On Experience:** Students and non-technical university personnel may lack the practical experience in identifying and avoiding phishing attacks.
- **Outdated Technology:** Due to a lack of resources universities often have to use outdated or inadequate technology infrastructure making it difficult to implement anti-phishing measures.
- **Resource Constraints:** Universities face resource constraints which can hinder implementing comprehensive phishing training programs.
- **Lack of Scalability:** Universities may encounter challenges in scaling their training initiatives to accommodate a growing student population.



# Day In The Life



# Current Process Flow



# University Collaboration

Phisecure's goal is to collaborate with universities to offer a unique educational experience.

With the Phisecure tool, Universities can provide a unique solution to teaching employees how to **identify** and **avoid** phishing scams.



# Solution Statement

Phisecure provides a customized training software solution, developing phishing **simulations** over a variety of platforms **tailored** to the user. The methods used during the simulation will be reported and explained in detail to the user. Creating a thorough **teaching** & **grading** process to help them identify phishing threats.

# Solution Characteristics

**Hands-On Experience:** Phisecure tool will simulate phishing attacks, so users can gain first hand experiences with this issue.

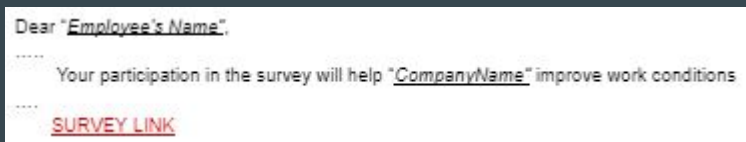
**Modern Technology:** The environments used for the simulation will be the popular technologies used in present day.

**Resource Management:** The process is automated, creating an effective training experience for the user, while only requiring their inputs.

**Scalability:** The software will not be restricted to only current technologies. It is intended to stay updated and adapt to newer technologies, as this will inevitably introduce new ways people can be attacked through phishing.

# Simulation

- The templates will be generated and designed via **Machine Learning**



- Attack variation is important, email is not the only **vulnerability**



- The attacks will be **randomized**. The time of the attacks and platforms will be unknown by the user

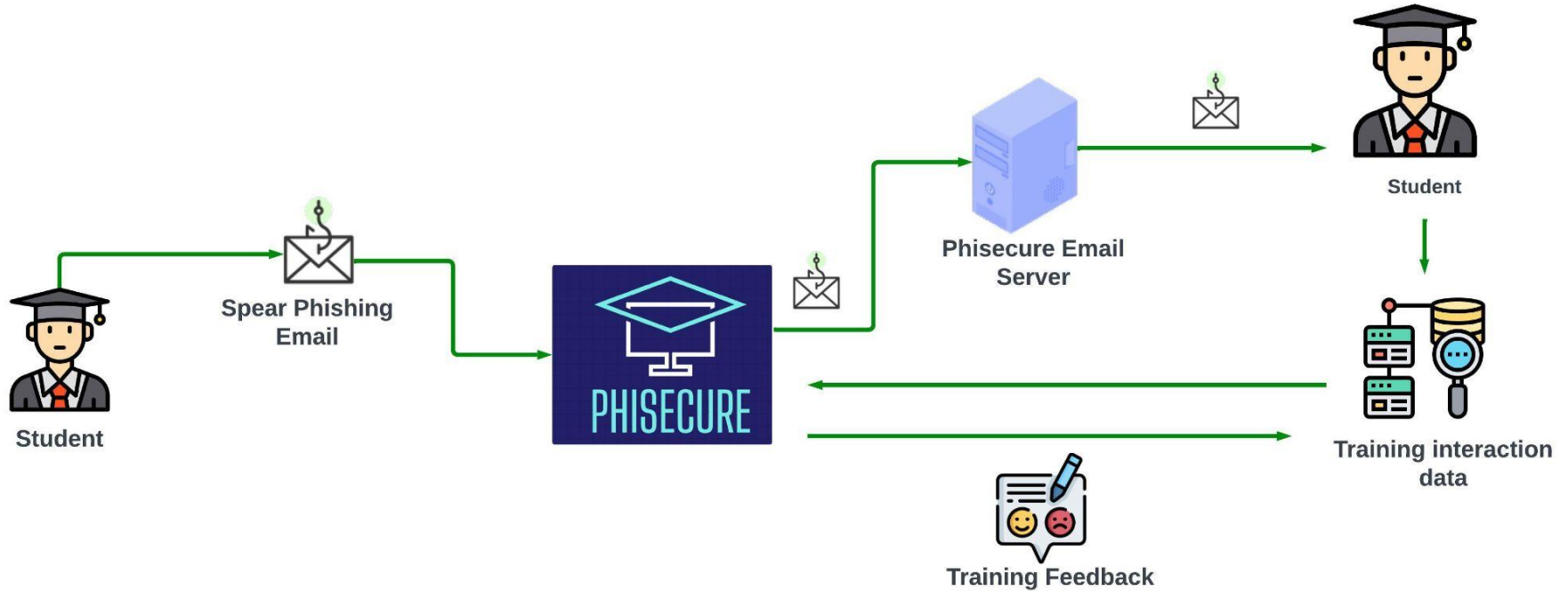
- The goal of the attacks will be to get interaction from the user in these forms
  - A reply back to the message, **exposing** personal information(**information will be deleted**)
  - Clicking a link that will imitate **Malware**. (**it will not be Malware**) The link will just report back that it was clicked.
  - If user detects that this is a malicious message, they are incentivised to reply "**SCAM**" for reports

# Feedback & Reports

- Feedback is given to the user after the **simulation** has been completed
- The user will be shown how well they performed
  - Did they spot the message and reply “**SCAM**”
  - Did they **expose** sensitive information
  - Did they click a **link** sent to them
- Phisecure will show the user what **red flags** they could have spotted
  - Were they asked to provide sensitive information
  - Was there unwarranted **urgency** or **threat**
  - Suspicious attachments sent
- All will be recorded for an overall progress report

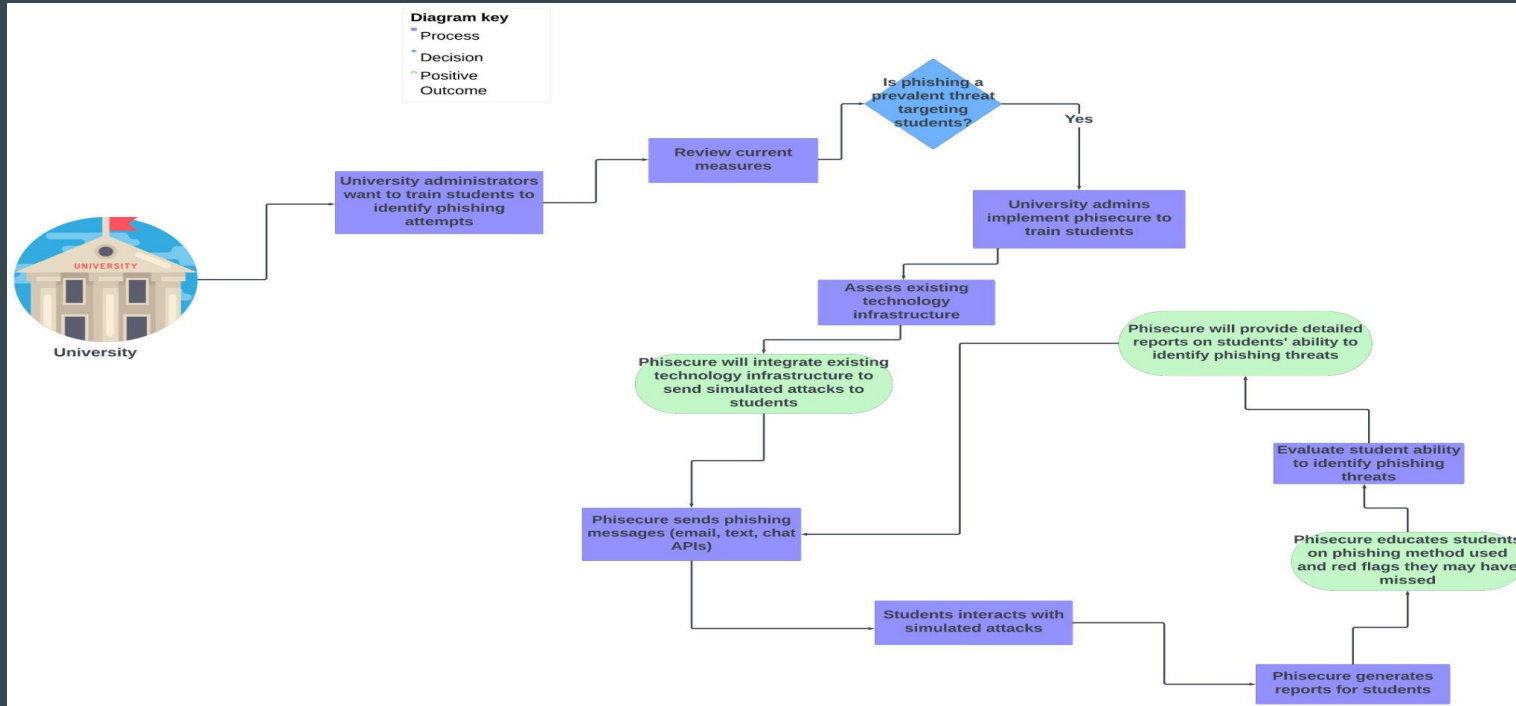
Links Clicked	Compromising replies	Successful Attacks	Most Successful Platform	Least Successful Platform
...	...	...	...	...

# Day In The Life (Solution)

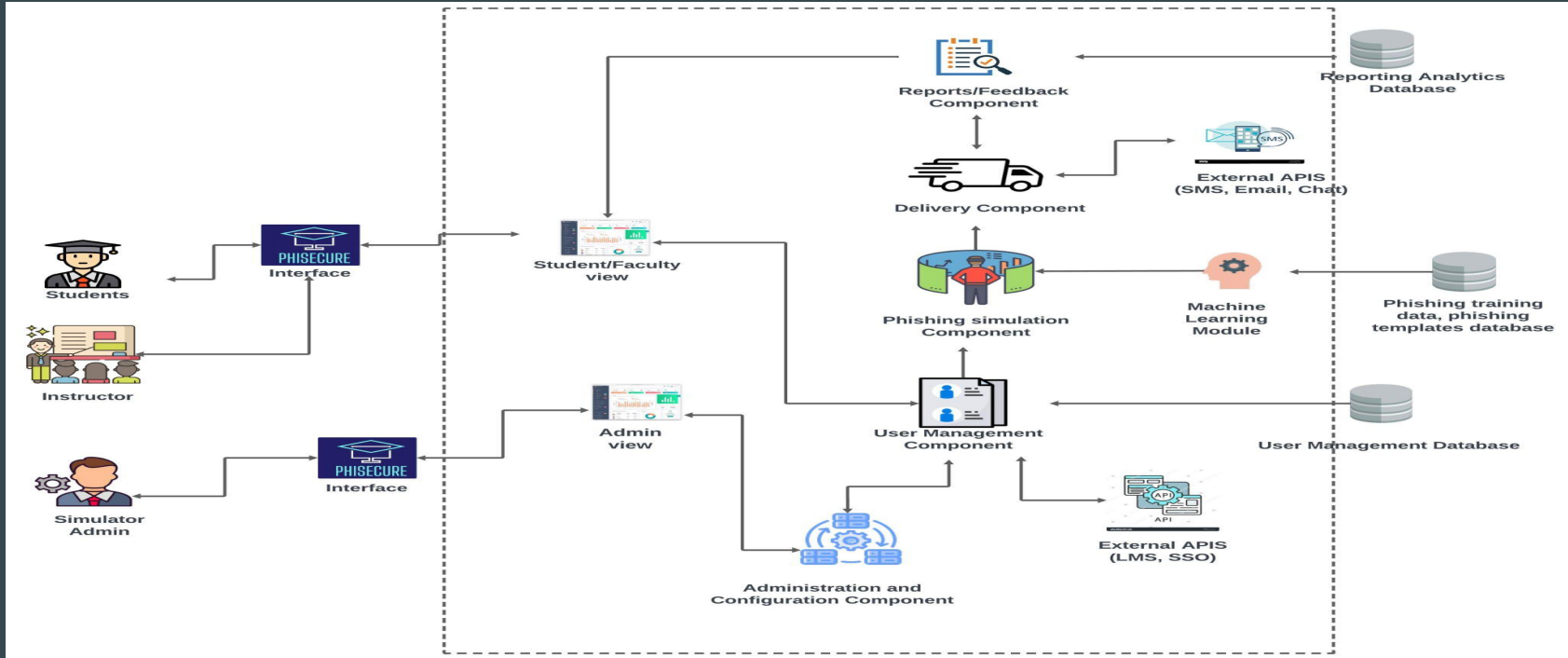




# Solution Process Flow



# Major Functional Component Design



# What does Phisecure do?

- **Simulate** realistic phishing attacks at the user
- **Customize** the training environment to match user's business environment
- **Educates** user on phishing methods
- **Instill** techniques that help mitigate chances of being phished

# What does Phisecure not do?

- Does not defend against phishing
- Will not alert user of a real phishing attack
- Cannot simulate the entire spectrum of phishing techniques

# Customers, End-Users, Stakeholders

## Customers:


- Universities

## End-Users:

- Students
- Instructor
- Simulator Administrators

## Stakeholders:

- University Leadership/Administrators (Deans, University Presidents )
- Employers

		Direct Competition				Indirect Competition
		Universities	Nice Challenge Project	Gophish	TrustedSec's Social Engineer Toolkit	KnowBe4
Free for Educational Institutions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMS Spoofing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Discord, Slack, and Microsoft Teams	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Designed for the Average User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Focus on Educating Targets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Peer Driven Spear Phishing	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Peer Training Effectiveness Assessment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

# Technical Risk Matrix

		Technical Risks				
		Impact				
Risk Matrix		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain			T3		
	Likely		T3			
	Possible			T1		T2
	Unlikely		T1		T2	
	Rare					

**T1.** Tool exposes sensitive information of users due to security vulnerabilities.

- Conduct regular security audits and penetration testing.
- Implement encryption protocols to protect user data.
- Provide secure authentication methods.

**T2.** Tool is susceptible to being hacked, leading to unauthorized access to user data.

- Employ strong security measures such as firewalls, intrusion detection systems, and access controls.
- Regularly update and patch software vulnerabilities.
- Implement multi-factor authentication.

**T3.** A lack of regular updates and maintenance may render the tool ineffective against evolving phishing techniques.

- Establish a maintenance schedule for updating content and addressing software vulnerabilities.
- Monitor emerging trends in phishing attacks and update the tool accordingly.

Technical Risks

Impact

Likelihood

Insignificant

Minor

Moderate

Major

Severe

Almost Certain

Likely

Possible

Unlikely

Rare

T1

T2

T3

# Customer Risk Matrix

Risk Matrix		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain					
	Likely		C3		C2	C1
	Possible	C3		C2	C5	C4
	Unlikely			C5	C1	C4
	Rare					

**C1.** Simulations within the education tool may not accurately reflect real-world phishing scenarios, leading to a disconnect between learning outcomes and practical application.

- Conduct thorough research to ensure simulations reflect current phishing techniques and trends accurately.
- Regularly update simulations to incorporate new phishing methods and tactics as they emerge.
- Solicit feedback from users to identify areas where simulations may be lacking or could be improved.
- Provide supplementary resources or exercises to reinforce learning and bridge any gaps between simulation and real-world scenarios.

**C2.** Users may not fully engage with the educational material, leading to ineffective learning.

- Design interactive and engaging content.
- Incorporate gamification elements to make learning enjoyable.
- Gather user feedback for continuous improvement.

**C3.** Users may feel overwhelmed or intimidated by the complexity of the tool, leading to disengagement

- Provide clear and intuitive user interfaces.
- Offer tutorials and support resources to assist users in navigating the tool.
- Conduct user testing to identify and address usability issues.

**C4.** Frequent exposure to simulated phishing attacks within the education tool may desensitize users to real-world threats.

- Implement varied and realistic phishing simulations to maintain user engagement and prevent desensitization.
- Provide ongoing education and reinforcement of phishing awareness best practices to remind users of the importance of remaining vigilant.
- Monitor user feedback and engagement metrics to identify signs of desensitization and adjust simulation frequency or intensity accordingly.
- Emphasize the dynamic and evolving nature of phishing threats to reinforce the need for continued vigilance and awareness.

**C5.** Users may develop a misleading perception that phishing is a static or predictable environment based on their interactions with the education tool.

- Provide clear messaging and educational content emphasizing the constantly evolving nature of phishing attacks.
- Incorporate real-world case studies and examples to illustrate the dynamic and adaptive tactics employed by cybercriminals.
- Encourage users to remain vigilant and proactive in staying informed about emerging phishing trends and techniques.
- Regularly update the education tool with new content and simulations that reflect current phishing landscape and trends.



# Legal Risk Matrix

Risk Matrix		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain					
	Likely		L2		L1	
	Possible			L1		
	Unlikely	L2				
	Rare					

## Legal Risks

**L1.** Legal and compliance issues could arise due to mishandling of user data or failure to meet regulatory requirements

- Comply with data protection laws such as GDPR, CCPA, etc.
- Obtain necessary permissions for data collection and processing.
- Implement privacy policies and terms of use

**L2.** Non-compliance with accessibility standards and regulations, leading to discrimination claims.

- Design and develop the tool following accessibility principles and guidelines (e.g., WCAG).
  - Conduct regular accessibility audits and testing.
- Provide accessible alternatives and accommodations for users with disabilities.

# Conclusion

- Phishing is a widespread issue that presents a significant challenge for universities.
- Phisecure offers a tailored solution, which provides customizable phishing simulations.
- Through collaboration with universities, Phisecure enhances its reach, offering innovative cybersecurity education.



# References

- 1) Irwin, Luke. "51 Must-Know Phishing Statistics for 2023: It Governance." *IT Governance UK Blog*, 19 June 2023, [www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023](http://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023).
- 2) "Top 10 Costs of Phishing - Hoxhunt." RSS, [www.hoxhunt.com/blog/what-are-the-top-10-costs-of-phishing#:~:text=Using%20different%20criteria%2C%20the%20Ponemon.as%20the%20king%20of%20cybercrime](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). Accessed 7 Feb. 2024.
- 3) Stansfield, Todd "Q3 2023 Phishing and Malware Report." *Q3 2023 Phishing and Malware Report*, Vade 15 Nov. 2023, [www.vadesecure.com/en/blog/q3-2023-phishing-malware-report#:~:text=in%20Q3%202023%2C%20Vade%20detected.180.4%20million](http://www.vadesecure.com/en/blog/q3-2023-phishing-malware-report#:~:text=in%20Q3%202023%2C%20Vade%20detected.180.4%20million).
- 4) "Cloudian Ransomware Survey Finds 65 Percent of Victims Penetrated by Phishing Had Conducted Anti-Phishing Training." Cloudian, [Victims Penetrated by Phishing Had Conducted Anti-Phishing Training \(cloudian.com\)](http://www.cloudian.com/victims-penetrated-by-phishing-had-conducted-anti-phishing-training)
- 5) Rezabek, Jeff. "How Much Does Phishing Cost Businesses?" *IRONSCALES*, IRONSCALES, 24 Jan. 2024, [ironscases.com/blog/how-much-does-phishing-cost-businesses](https://www.ironscases.com/blog/how-much-does-phishing-cost-businesses).
- 6) "Must-Know Phishing Statistics - Updated for 2024: Egress." *Egress Software Technologies*, Egress Software Technologies, 19 Jan. 2024, [www.egress.com/blog/phishing/phishing-statistics-round-up](http://www.egress.com/blog/phishing/phishing-statistics-round-up).
- 7) Sheng, Ellen. "Phishing Scams Targeting Small Business on Social Media Including Meta Are a 'gold Mine' for Criminals." *CNBC*, CNBC, 15 Aug. 2023, [www.cnbc.com/2023/08/15/gold-mine-phishing-scams-rob-main-street-on-social-media-like-meta.html](http://www.cnbc.com/2023/08/15/gold-mine-phishing-scams-rob-main-street-on-social-media-like-meta.html).
- 8) "Cybersecurity Training and Certifications." *Infosec*, [www.infosecinstitute.com/](http://www.infosecinstitute.com/). Accessed 10 Feb. 2024.
- 9) Michelle Steves, Kristen Greene, Mary Theofanos, Categorizing human phishing difficulty: a Phish Scale, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa009, <https://doi.org/10.1093/cybsec/tyaa009>
- 10) *Hoxhunt for End Users*, [support.hoxhunt.com/hc/en-us/categories/360000079772-Hoxhunt-for-end-users](http://support.hoxhunt.com/hc/en-us/categories/360000079772-Hoxhunt-for-end-users). Accessed 10 Feb. 2024.
- 11) KnowBe4. "Security Awareness Training." *KnowBe4*, [www.knowbe4.com/](http://www.knowbe4.com/). Accessed 10 Feb. 2024.
- 12) Steves, Michelle, et al. "Categorizing Human Phishing Difficulty: A Phish Scale." *OUP Academic*, Oxford University Press, 14 Sept. 2020, [academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453](http://academic.oup.com/cybersecurity/article/6/1/tyaa009/5905453).
- 13) *Nice Challenge Project*, [nice-challenge.com/](http://www.nice-challenge.com/). Accessed 25 Feb. 2024.
- 14) "Phishing - Glossary: CSRC." *CSRC Content Editor*, NIST, [csrc.nist.gov/glossary/term/phishing](https://csrc.nist.gov/glossary/term/phishing). Accessed 29 Feb. 2024.
- 15) Paun, Goran. "Council Post: Building a Brand: Why a Strong Digital Presence Matters." *Forbes*, Forbes Magazine, 20 Feb. 2024, [www.forbes.com/sites/forbesagencycouncil/2020/07/02/building-a-brand-why-a-strong-digital-presence-matters/?sh=31cb7e249f26](https://www.forbes.com/sites/forbesagencycouncil/2020/07/02/building-a-brand-why-a-strong-digital-presence-matters/?sh=31cb7e249f26)
- 16) Smith, Gary. "Top Phishing Statistics for 2024: Latest Figures and Trends." *StationX*, StationX, 16 Feb. 2024, [www.stationx.net/phishing-statistics/](http://www.stationx.net/phishing-statistics/).
- 17) 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-cybercams-targeting-students](http://www.insidehighered.com/news/students/safety/2023/07/18/universities-warn-increased-cybercams-targeting-students).
- 18) "What Is Cybersecurity?" *Cisco*, Cisco, 22 Feb. 2024, [www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html](http://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html).

# Glossary and Appendices

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.