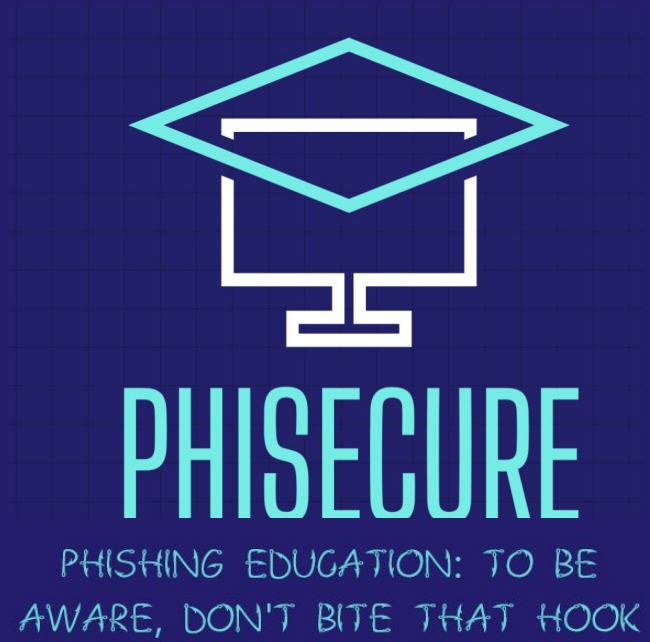


CS411W Final Demo Presentation

By: Team Orange (2024)

12/12/24

Table of Contents

Team Members

Team Leader

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.

Frontend Lead

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

Webmaster

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

Backend Lead

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.

Database Lead

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.

Phishing - A Growing Threat

- 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![16]
  - **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!
  - To demonstrate this problem, let's look at a recent attack from an educational institution to demonstrate why this is a problem...

A Case Study in Phishing Vulnerability

- Students at California State University 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.[17]
- 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.

A Case Study in Phishing Vulnerability (cont.)

- **82** student accounts of theirs were compromised in Q2 of 2023, up from almost zero at the beginning of 2021.[17]
- 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).
- This proves to be a massive challenge for universities to mitigate and prevent attacks like this. Why?

Phishing: A Growing Threat

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

Phishing Education

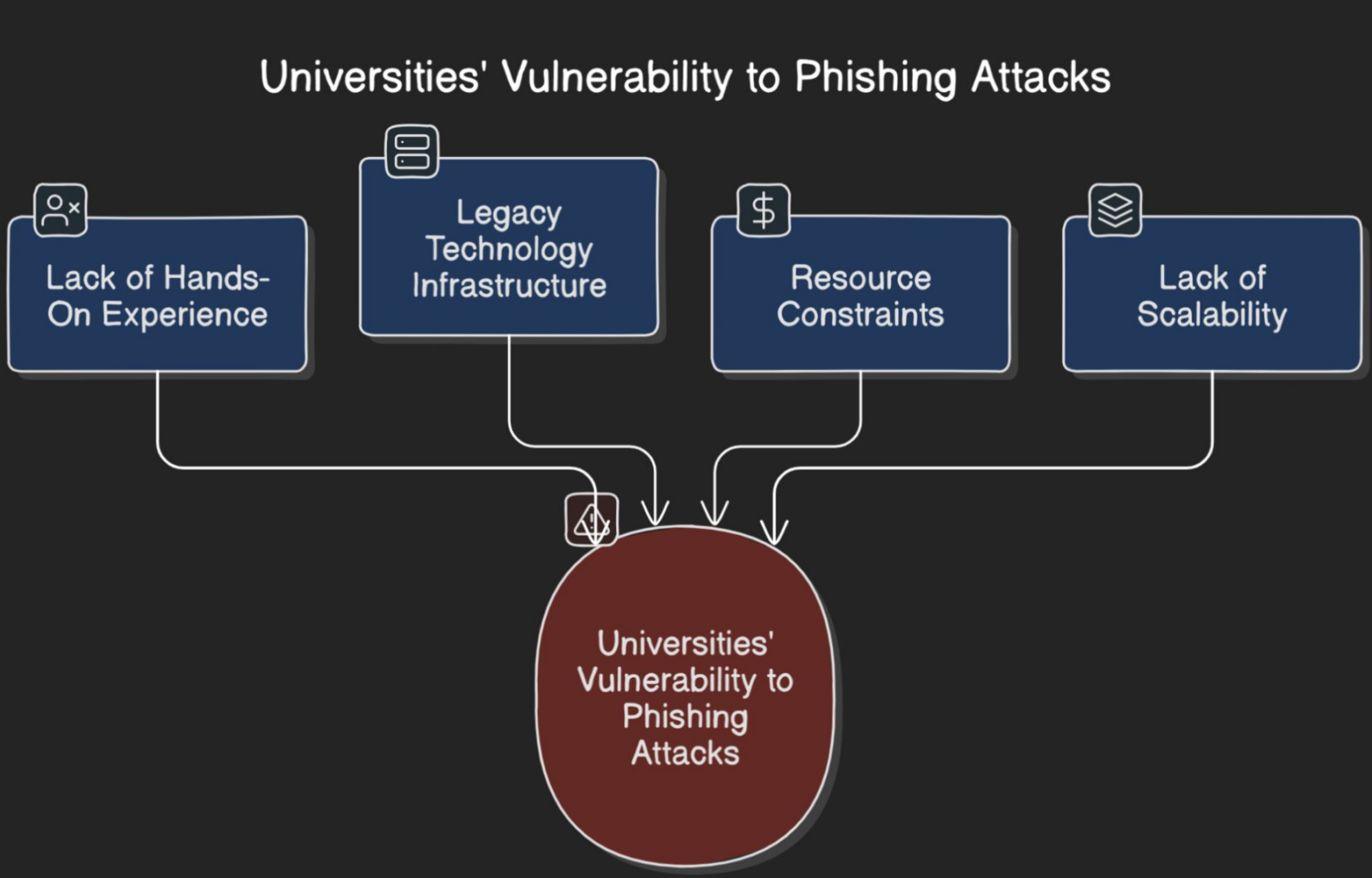
It's becoming more and more clear students and faculties at these universities do not have the proper training required to discern phishing scams from legitimate emails

- The average click rate for a phishing attack is **17.8%** , going to to **53.2%** for more targeted spear phishing attacks![16]
- 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.
- **Legacy Technology Infrastructure:** Due to resource constraints universities may rely on inadequate technology infrastructure which can impact students' learning experiences.
- **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.


Universities' Vulnerability to Phishing Attacks
Lack of Hands-On Experience
Legacy Technology Infrastructure
Resource Constraints
Lack of Scalability
Universities' Vulnerability to Phishing Attacks

Solution Statement

Phisecure provides a customized training software solution, developing phishing simulations that are 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.

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 students how to identify and avoid phishing scams.

Solution Characteristics

Hands-On Experience: Phisecure offers personalized phishing simulations, giving users a firsthand experience with realistic phishing scenarios and insightful feedback related to the interaction via the Dashboard Module

Modern Technology: Using the User Personalization Component, users will experience modern day phishing methods referencing popular services that they use for the simulations.

Resource Management: Automates the process with minimal setup using the User Management Module and automates the performance feedback that is displayed in the Dashboard Module.

Scalability: Phisecure ensures scalability through the Peer Phishing Component, allowing users to help with creation of new and unique phishing templates. Combined with the User Management Module, it simplifies onboarding and role-based access, making it easy to scale for larger groups

Simulation

- Personalized templates will be selected that relate to the user

- User Personalization Component ensures the contents of the messages will relate to the user as well
- The time of the attacks will be unknown by the user
- The goal of these 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 report the message.

Dashboard Module

- The Phisecure Performance Dashboard provides users with feedback on their performance following the simulation.
- The user will be shown how well they performed
  - Did they spot the message and report it
  - Did they expose sensitive information
  - Did they click a link sent to them
- Phisecure will use the Red Flag Recognition Feature to 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 performance data is recorded and visualized in the Dashboard for overall progress tracking

Peer Phishing Component

- Students will select another student for a simulated attack

- Students will create a template for phisecure to use

- Success of their attack will be recorded and reported to them (no sensitive information will be shared)

Purpose of Feature

  - This can promote more interaction and a different perspective
  - Successful templates can be adapted into Phisecure's template database for future use

Customers, End-Users, Stakeholders

Customers:

- Universities

End-Users:

- Students
- Instructor
- Simulator Administrators

Stakeholders:

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

MFCD Breakdown

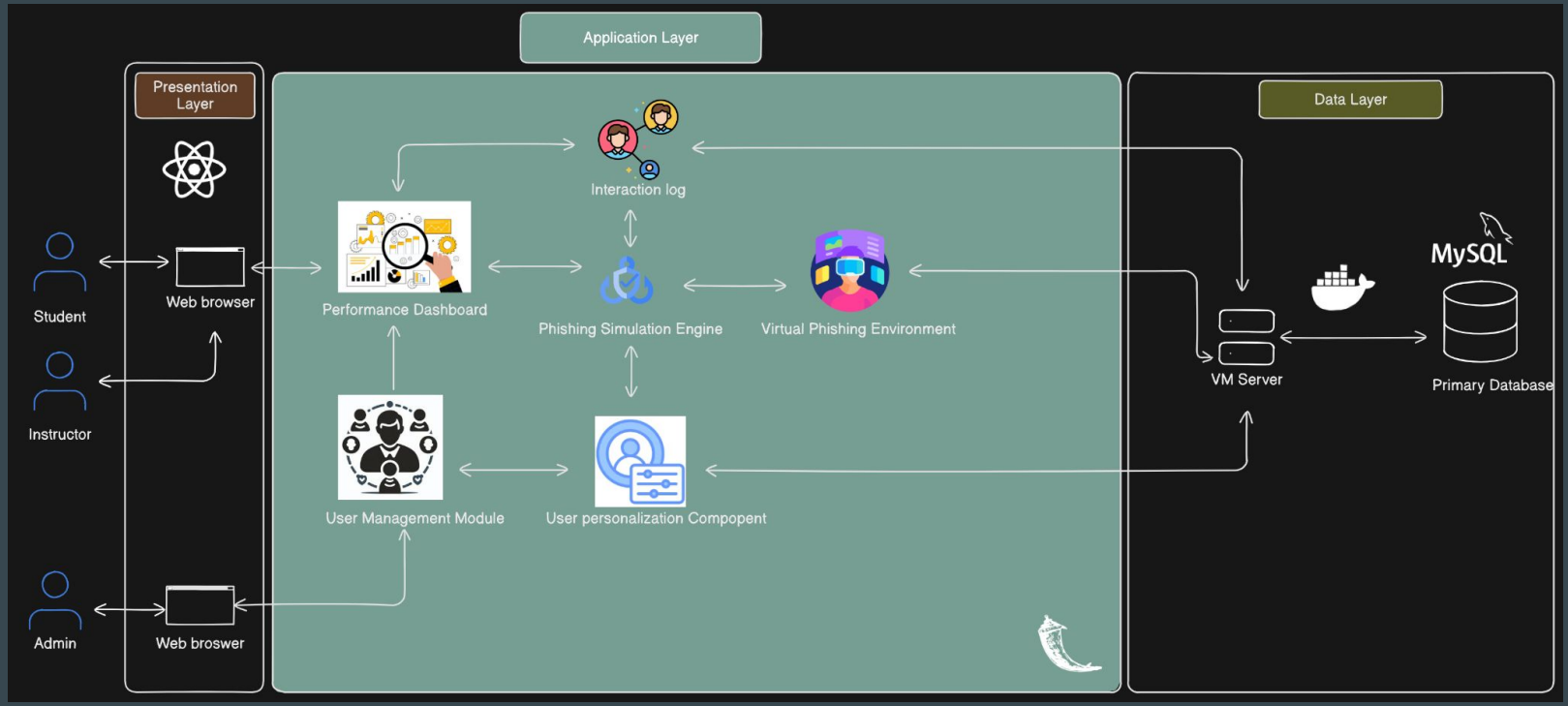
Components/Modules:

- Phisecure Performance Dashboard: Provides users with personalized feedback based on interactions with phishing templates.
- Phishing Simulation Engine: Creates a variety of phishing scenarios for student to interact with.
- User Personalization Component: Tailors phishing email templates based on user questionnaire and previous simulation encounters
    - Adjusts the difficulty of phishing emails based on user performance.
- Virtual phishing environment: Simulates regular email inbox where students interact with phishing emails.
- User management Module: Handles user creation and role-based access control.

Infrastructure:

Hosting Environment: ODU provided VM using docker.

Prototype Major Functional Component Design



RWP Vs Prototype

Category	Features	RWP	Prototype	Reason for Partial Implementation/Drop
User Management	Account Creation	Fully Functional	Fully Functional	
	Login using University Credentials	Fully Functional	Not Implemented	Creating our own built in virtual email client environment
	Instructor Course management	Fully Functional	Fully Functional	
	Role-Based Access Control	Fully Functional	Fully Functional	
Phishing simulation	Personalized Phishing Templates	Fully Functional	Fully Functional	
	Email phishing simulation scenarios	Fully Functional	Fully Functional	
	SMS phishing simulation scenarios	Fully Functional	Not Implemented	Creating our own built in virtual email client environment
	Live chat phishing simulation scenarios	Fully Functional	Not Implemented	Creating our own built in virtual email client environment
	Attack time settings	Fully Functional	Fully Functional	
	Peer to Peer phishing	Fully Functional	Partial Functional	Focused primarily email phishing simulation and personalization
	Questionnaire	Fully Functional	Fully Functional	
	Interactive Tutorial	Fully Functional	Not Implemented	Focused on implementing core features. github wiki contains user manual
Feedback/Reports	Red Flag Recognition	Fully Functional	Fully Functional	
	Student interaction report	Fully Functional	Fully Functional	
	Class performance report	Fully Functional	Fully Functional	
	Instructor feedback	Fully Functional	Fully Functional	
	Most Successful Platform	Fully Functional	Partial Functional	Only using email for prototype
	Least Successful Platform	Fully Functional	Partial Functional	Only using email for prototype
Phisecure Performance Dashboard	Simulation result summary	Fully Functional	Fully Functional	
	Overall Risk assesment score	Fully Functional	Fully Functional	
	Student dashboard	Fully Functional	Fully Functional	
	Instructor dashboard	Fully Functional	Fully Functional	
	Template peformance graphs	Fully Functional	Fully Functional	
	Role based dashboard	Fully Functional	Fully Functional	

RWP Vs Prototype

Virtual Phishing environment	Inbox simulator	Not Implemented	Fully Functional	RWP will integrate with actual university email
	Email Servers	Fully Functional	Not Implemented	focused on interactive inbox simulation in virtual phishing environment
	Web Servers	Fully Functional	Not Implemented	focused on interactive inbox simulation in virtual phishing environment
	Domain Setup	Fully Functional	Not Implemented	focused on interactive inbox simulation in virtual phishing environment
	Network Isolation	Fully Functional	Not Implemented	focused on interactive inbox simulation in virtual phishing environment
Analytics	Click rate	Fully Functional	Fully Functional	
	Open rate	Fully Functional	Fully Functional	
	Reply rate	Fully Functional	Fully Functional	

Software/Hardware Tools

- Frontend
  - Framework: React
  - Languages: Javascript, HTML, CSS
  - IDE: VS Code
- Backend
  - Framework: Flask
  - Languages: Python
  - IDE: VS Code
- Database
  - MySQL
- Repository/Version Control Tools
  - Git and GitHub

User Story: Student

- As a Student, I need the ability to perform my own phishing attacks against my peers.
- As a Student, I need to acquire feedback about phishing attacks I fell for so that I may better understand where I could learn to avoid said attack in the future.
- As a Student, I need to be graded on the success of my created attacks
- As a Student, I need to be graded on my ability to recognize an attack created by other students
- As a Student, I need to be shown the red flags I could have spotted
- As a Student, I want the UI to be easy to navigate

User Management	Phishing Simulation	Feedback/Reports	User Interface	Virtual Phishing Environment	Analytics	Other

User Story: Admin

- As an administrator, I need to manage user accounts, which include registration, authentication, and permissions management.
- As a simulator admin, I want to have access to user management configuration where I can assign roles and permissions to individual users, including the ability to launch simulated phishing attacks.
- As an administrator, I need to be able to see an assessment on how effective a phishing attack was.
- As a simulator admin, I want to have access to a dashboard or interface where I can view aggregated data and analytics on user interactions with simulated phishing attacks .
- As an administrator, I need the student information given to Phisecure to be protected from outside agents.
- As an Administrator, I need to monitor system usage and performance to ensure optimal functionality.

User Management	Phishing Simulation	Feedback/Reports	User Interface	Virtual Phishing Environment	Analytics	Other

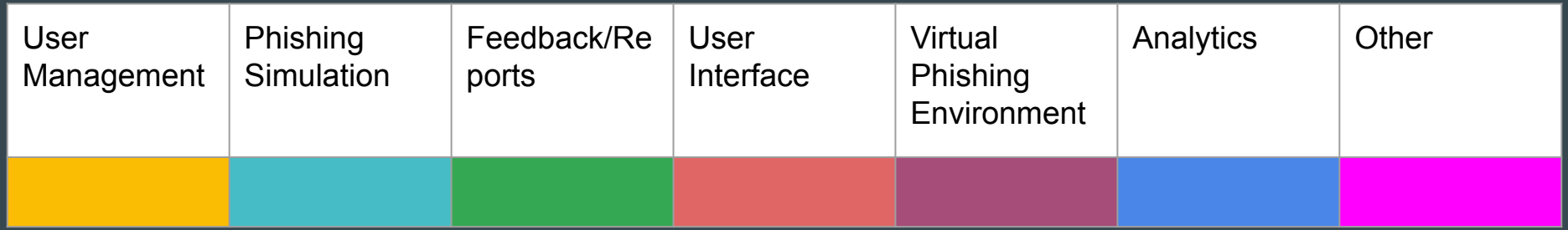
User Story: Instructor

- As an Instructor, I need to have the ability to add, remove, and modify student data for my class through Phisecure
- As an Instructor, I need the phishing attacks to be personalized to promote interaction from the students
- As an Instructor, I need to know if the student successfully avoided a phishing attack or if they never saw it
- As an Instructor, I need to monitor my students through Phisecure
- As an Instructor, I need to see links that my students clicked
- As an Instructor, I need to see the student's Phisecure grade
- As an Instructor, I want to be able to control when the attacks will occur

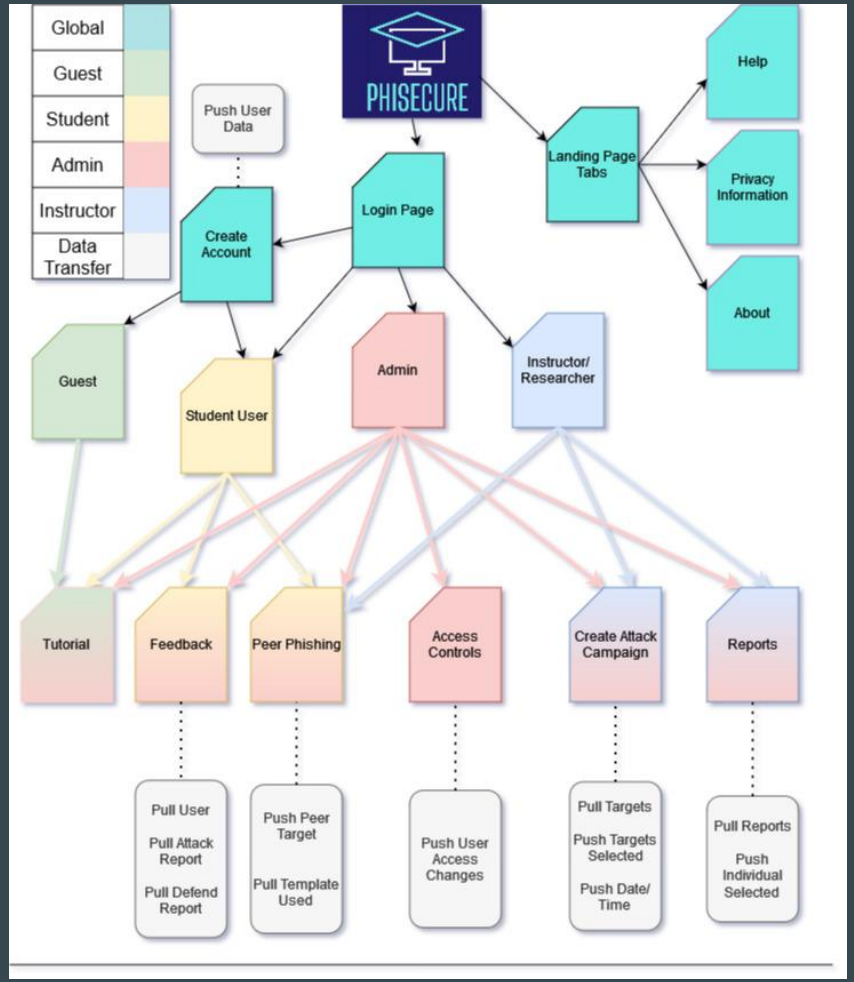
User Management	Phishing Simulation	Feedback/Reports	User Interface	Virtual Phishing Environment	Analytics	Other

User Story: Tester

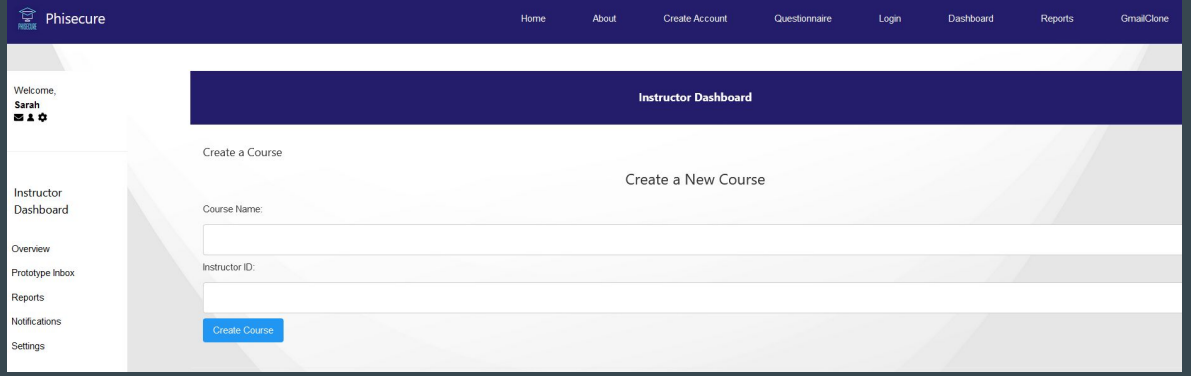
- As a tester, I want to be able to create and manage student accounts to simulate classes for testing purposes
- As a tester, I need to be able to access admin rights
- As a tester, I want to be able to create/delete an account
- As a tester, I want to be able to create a simulation against myself to verify functionality
- As a tester, I would like to send myself feedback based on my selected role to verify functionality
- As a tester, I want to validate user interface elements for consistency, usability, and accessibility.
- As a tester, I want to be able to run unit, integration, and system tests
- As a tester, I want to be performing incremental testing each sprint.
- As a tester, I need a webpage to analyze links clicked.

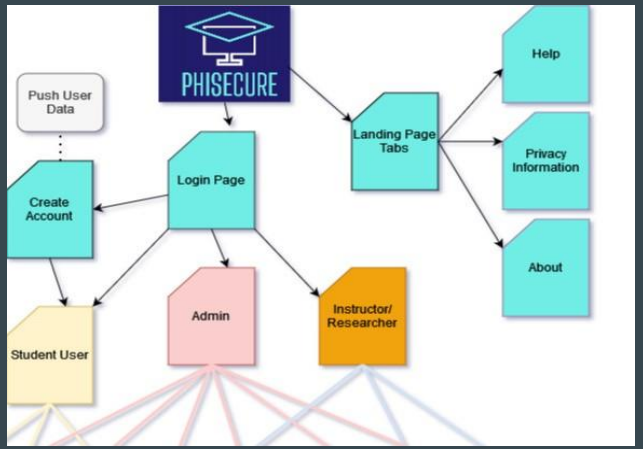


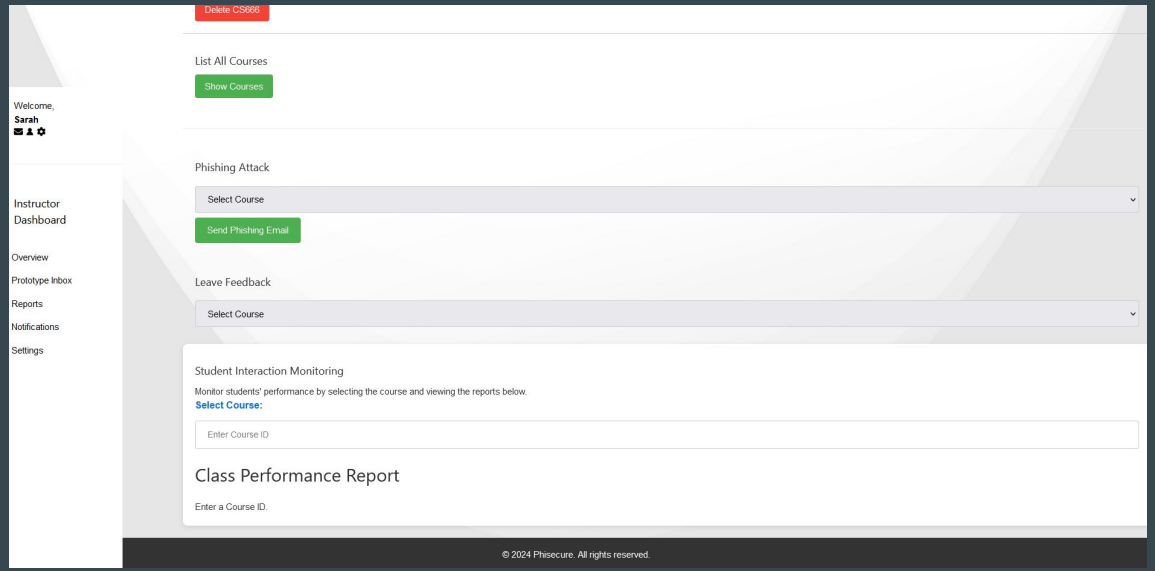
User Interface Sitemap

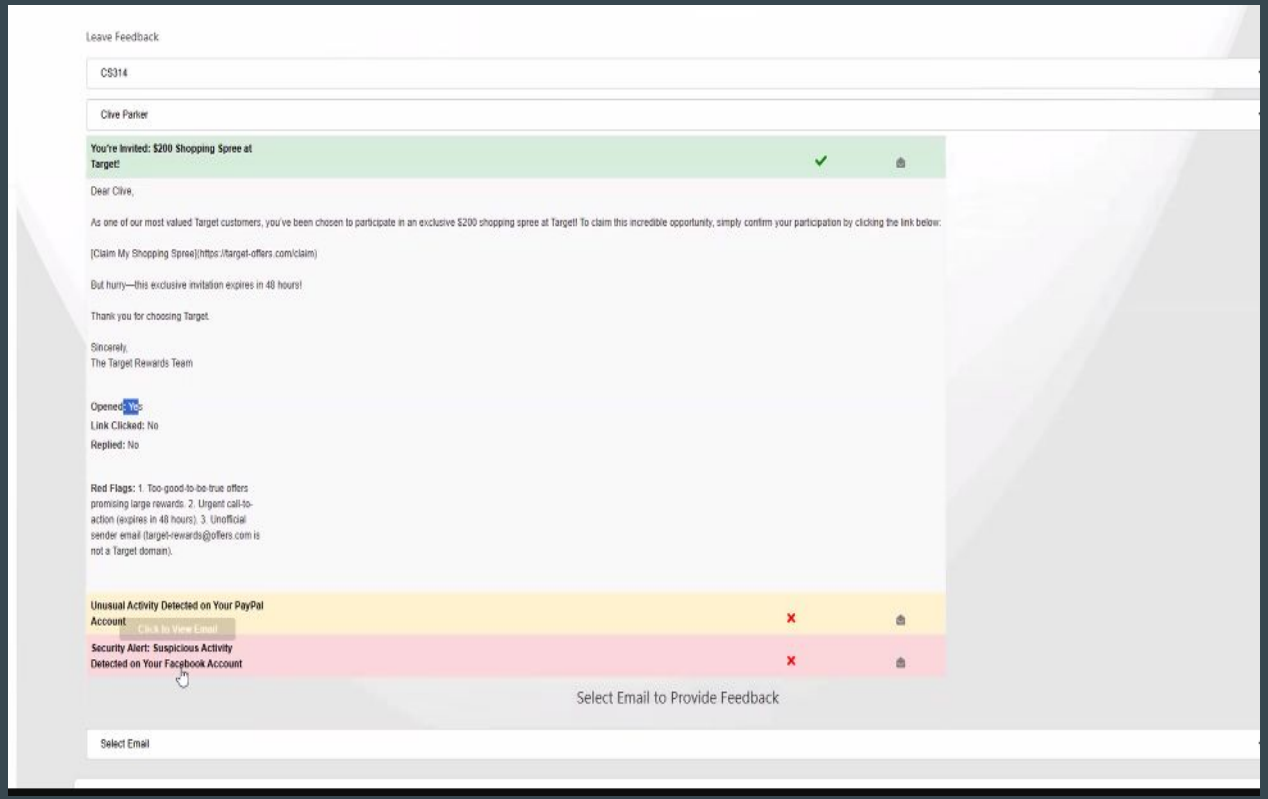


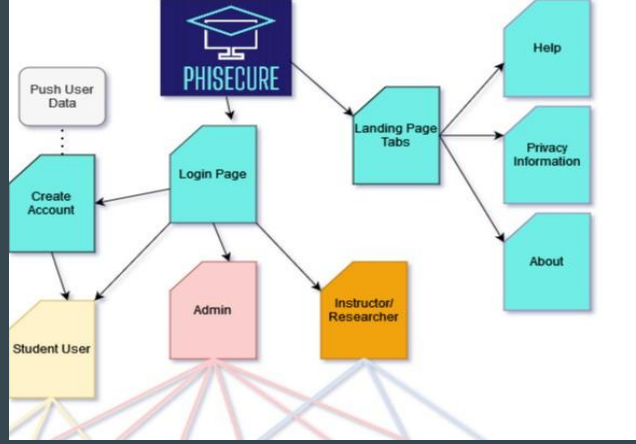
Instructor User



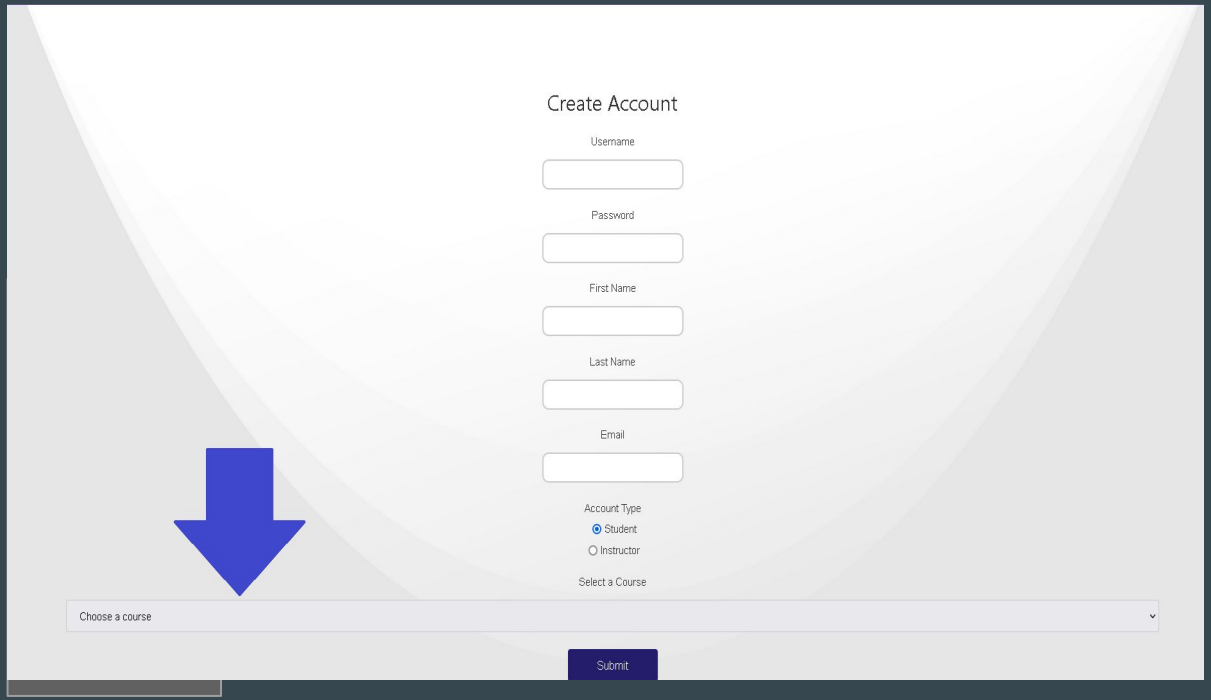


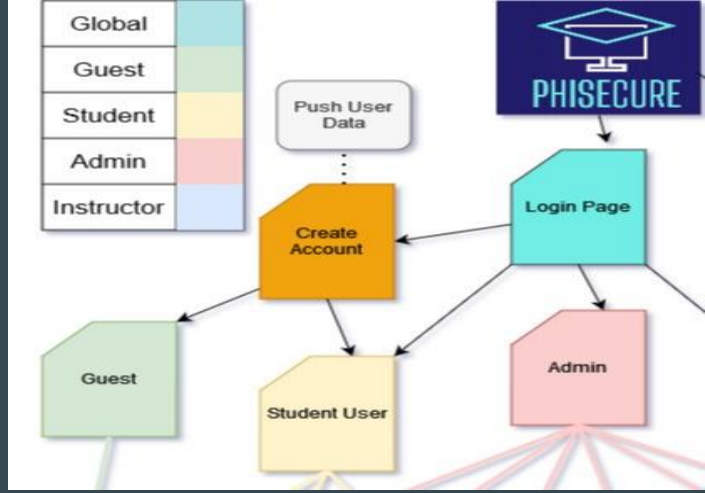






Instructor User





Student Users

Phisecure

Home About Create Account Questionnaire Login Dashboard Reports GmailClone

Phisecure Questionnaire

questionnaire for new users

Question 1: Has your college and/or place of employment recently suffered a wide-scale spear phishing attack?

Yes No

Question 2: How often do you change your password?

Every month Every 3 months Every 6 months Once a year Never

Question 3: Do you reuse passwords for multiple accounts?

Yes No

Question 4: Do you check the senders email address before clicking on links or replying to emails?

Yes No

Question 5: Do you shop online? If yes, which platforms do you use most?

Amazon eBay Walmart Target Other retail websites I don't shop online

Question 6: Do you manage your finances online? Which platforms do you use?

Banking apps PayPal Venmo Cash App Investment platforms I don't manage finances online

Question 7: Which work or school-related tools do you use frequently?

Microsoft Office 365 Google Workspace Zoom Slack Microsoft Teams Other

Question 8: What type of email are you most likely to open immediately?

Work/School related Personal correspondence Shopping/Retail Financial notifications Social media notifications

Question 9: What social media services do you use?

Facebook Twitter/X Instagram LinkedIn TikTok None

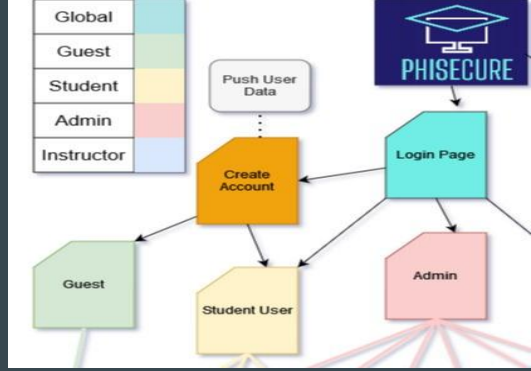
Question 10: Are you currently employed? if so enter the name of your employer (if your not employed simply enter N/A)

Enter your answer here...

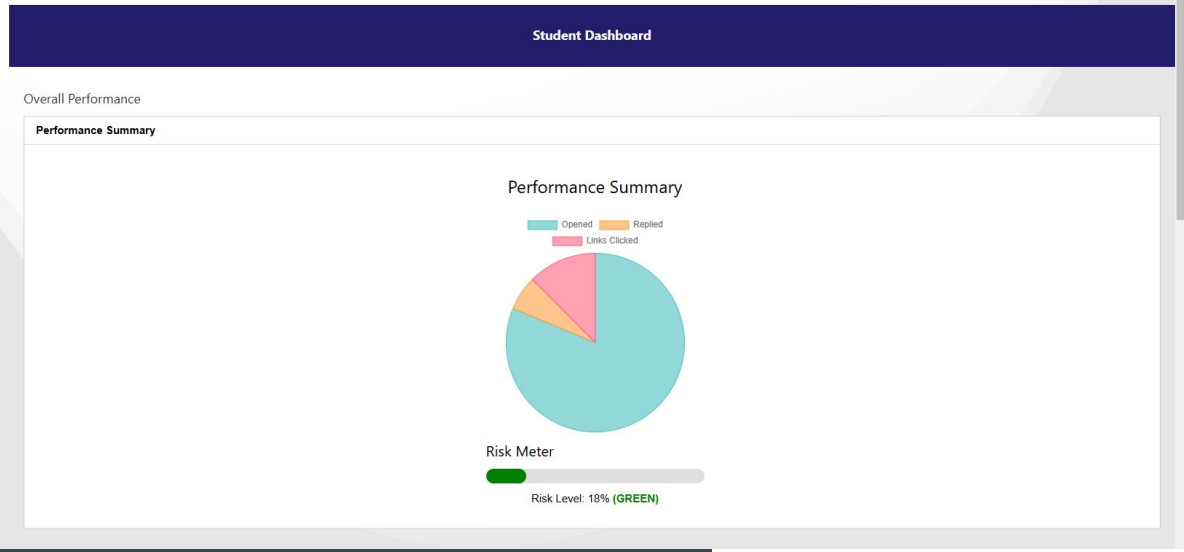
Question 11: What is your major? (if you are undecided enter undecided)

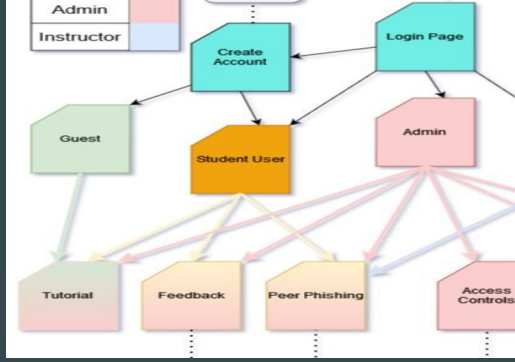
Enter your answer here...

Submit



Student Users





Student Users

Phishing Email Feedback

Email Title	Reviewed	Feedback
Urgent: Billing Issue on Your Venmo Account - Action Required	✗	
Action Required: Validate Your Microsoft Office 365 Subscription	✗	
Urgent: Action Required to Verify Your Zoom Account	✗	
Your $50 eBay Loyalty Reward is Waiting!	✗	
Your $100 Walmart Shopping Voucher Awaits!	✗	
Action Required: Important Update to Your Slack Account	✗	
Congratulations! You've Won a $100 Gift Card	✗	
Delivery Attempt Failed - Action Required	✗	
Alert: Suspicious Login Detected on Your Account	✗	

Phisecure

Home | About | Create Account | Questionnaire | Login | Dashboard | Reports | GmailClone | Phise

Peer Phishing Template

Template Name:

Enter template name

Subject:

Enter subject template

Template Description:

Enter template description

Red Flag:

Enter a red flag

Template Category:

Enter template category

Difficulty Level:

- Beginner
- Intermediate
- Advanced

Sender:

Enter sender's email

Available Tags

{first_name}

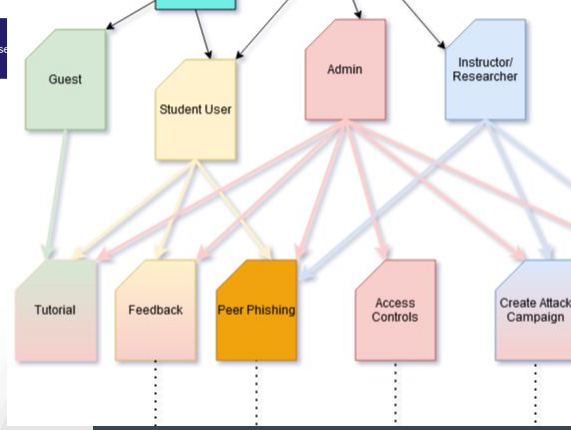
{last_name}

{date}

Email Body

B I U S {} x² x₂ Normal T Font

Create and Send



Technical Risk Matrix

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. The school's email security measures may mistakenly identify the simulated phishing emails as threats and block them before they reach the students' inboxes.

- Engage with the school's IT department to inform them about the simulated phishing campaign and its educational purpose. Provide details about the sender email addresses and content to prevent blocking.
- Request the school's IT department to whitelist the sender email addresses or domains used for sending simulated phishing emails to ensure they are not blocked by email filters.

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.

Customer Risk Matrix

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. 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.

C3 Some students may misuse the phishing simulation platform to launch real phishing attacks against their peers instead of participating in the educational exercise as intended.

- Establish clear guidelines and policies outlining acceptable use of the phishing simulation platform. Clearly communicate the consequences of engaging in malicious activities
- Monitor user activity on the platform to detect any suspicious behavior or unauthorized actions, such as unusual patterns of email sending or targeting specific individuals
- Educate students about the ethical and legal implications of engaging in malicious activities, emphasizing the importance of responsible behavior in cybersecurity practices
- Immediately suspend or revoke access privileges for any student found engaging in malicious activities, and notify appropriate authorities or school administration if necessary. Provide support and guidance to affected students and take corrective actions to mitigate any damage caused.

Legal Risk Matrix

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.
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. 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).
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)
5) Rezabek, Jeff. “How Much Does Phishing Cost Businesses?” *IRONSCALES*, IRONSCALES, 24 Jan. 2024, ironscales.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.
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.
8) “Cybersecurity Training and Certifications.” *Infosec*, 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. Accessed 10 Feb. 2024.
11) KnowBe4. “Security Awareness Training.” *KnowBe4*, 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.
13) *Nice Challenge Project*, nice-challenge.com/. Accessed 25 Feb. 2024.
14) “Phishing - Glossary: CSRC.” *CSRC Content Editor*, NIST, 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
16) Smith, Gary. “Top Phishing Statistics for 2024: Latest Figures and Trends.” *StationX*, StationX, 16 Feb. 2024, 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-cyberscams-targeting-students.
18) “What Is Cybersecurity?” *Cisco*, Cisco, 22 Feb. 2024, 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.