



PHISECURE

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

CS410 Prototype Presentation

By: Team Orange (2024)

4/18/24

Table of Contents

3-5. [Team Members](#)

6-7. [The Problem](#)

8-12. [The Solution: Phisecure](#)

13. [Phisecure: Its uses and its Users](#)

14-15. [What the prototype will implement](#)

16. [Major Functional Component Design](#)

17-18. [Hardware/Software and Testing](#)

19-22. [User Stories](#)

23. [Sprint Breakdown](#)

24-26. [Risk Matrix](#)

27. [Conclusion](#)

28. [References](#)

29. [Glossary](#)

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.



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.



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.

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.

Solution Characteristics

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

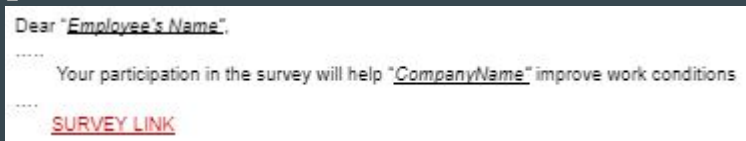
Modern Technology: The environments used for the simulation will be the popular technologies used in present day.

Resource Management: The process is automated, creating an effective training experience for the user, while only requiring introductory inputs in the beginning stage.

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 selected that relate to the user



Dear "Employee's Name",
.....
Your participation in the survey will help "CompanyName" improve work conditions
.....
[SURVEY LINK](#)

- The attacks will be **randomized**. The time of the attacks 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

Peer Phishing

- 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

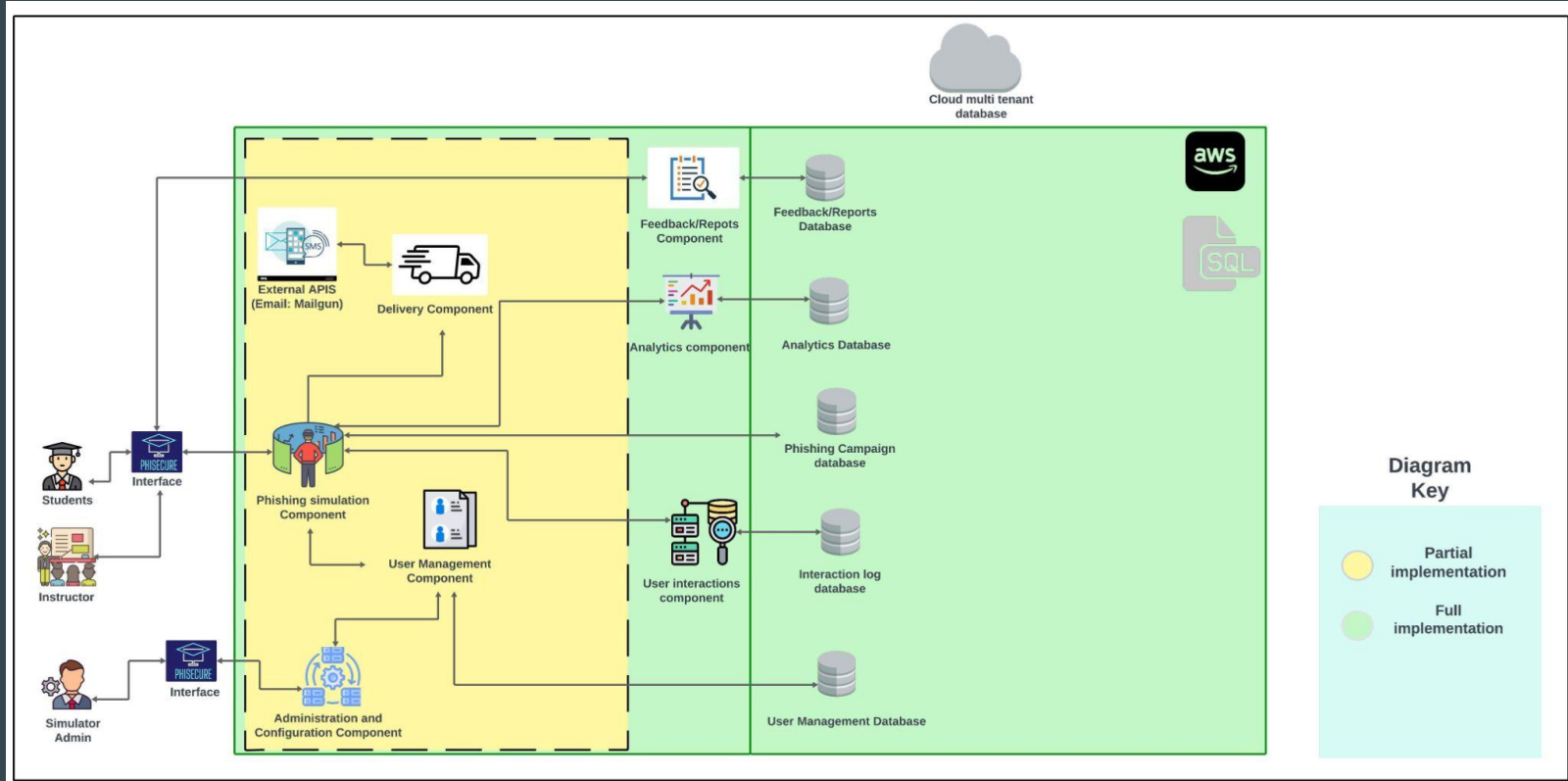
RWP Vs Prototype

| Category | Features | RWP | Prototype | Reason for Partial Implementation/Drop |
|-----------------------------|------------------------------------|----------------------|-----------------------------------------------------|----------------------------------------------------------------------------|
| User Account Management | User Registration | Fully functional | Fully functional | |
| | Account Creation/Deletion | Fully functional | Fully functional | |
| | Login using University Credentials | Fully functional | Not Implemented | Going to use fake accounts for prototype |
| | Role-Based Access Control | Fully functional | Fully functional | |
| Phishing Simulation | Generate a Custom Phishing Attack | Fully functional | Fully functional | |
| | Send Phishing Attack via Email | Fully functional | Fully functional | |
| | Send Phishing Attack via SMS | Fully functional | Not Implemented | Only focusing on email for prototype |
| | Send Phishing Attack via Live Chat | Fully functional | Not Implemented | Only focusing on email for prototype |
| | ML Generated Templates | Not Implemented | Not Implemented | ML dropped due to overcomplication of the project |
| | Tutorial | Fully functional | Paritally functional | Will be a prototype tutorial, so it will be missing features not yet added |
| | Peer Phishing | Fully functional | Paritally functional | Will only be able to attack through email |
| | Attack time Settings | Fully functional | Fully functional | |
| Attack Environment Settings | Fully functional | Paritally functional | Only one environment will be possible for selection | |
| Feedback/Reports | Red Flags Missed | Fully functional | Fully functional | |
| | Links Clicked | Fully functional | Fully functional | |
| | Compromising | Fully functional | Fully functional | |
| | Successful Attacks | Fully functional | Fully functional | |
| | Most Successful Platform | Fully functional | Not Implemented | Only using email for prototype |
| | Least Successful Platform | Fully functional | Not Implemented | Only using email for prototype |

RWP Vs Prototype

| Category | Features | RWP | Prototype | Reason for Partial Implementation/Drop |
|--------------------------------|------------------------------|------------------|------------------|------------------------------------------------------------------|
| User Interface | Admin Dashboard | Fully functional | Fully functional | |
| | Student/Instructor Dashboard | Fully functional | Fully functional | |
| | Home Page | Fully functional | Fully functional | |
| Sandboxed Phishing Environment | Email Servers | Fully functional | Not implemented | Not implementing the researcher testing environment in prototype |
| | Web Servers | Fully functional | Not implemented | Not implementing the researcher testing environment in prototype |
| | Domain Setup | Fully functional | Not implemented | Not implementing the researcher testing environment in prototype |
| | Network Isolation | Fully functional | Not implemented | Not implementing the researcher testing environment in prototype |
| Analytics | Click rate | Fully functional | Fully functional | |
| | Disclosure rate | Fully functional | Fully functional | |
| | Reporting of attack rate | Fully functional | Fully functional | |
| | Interaction rate | Fully functional | Fully functional | |
| | Time-to-Response | Fully functional | Fully functional | |

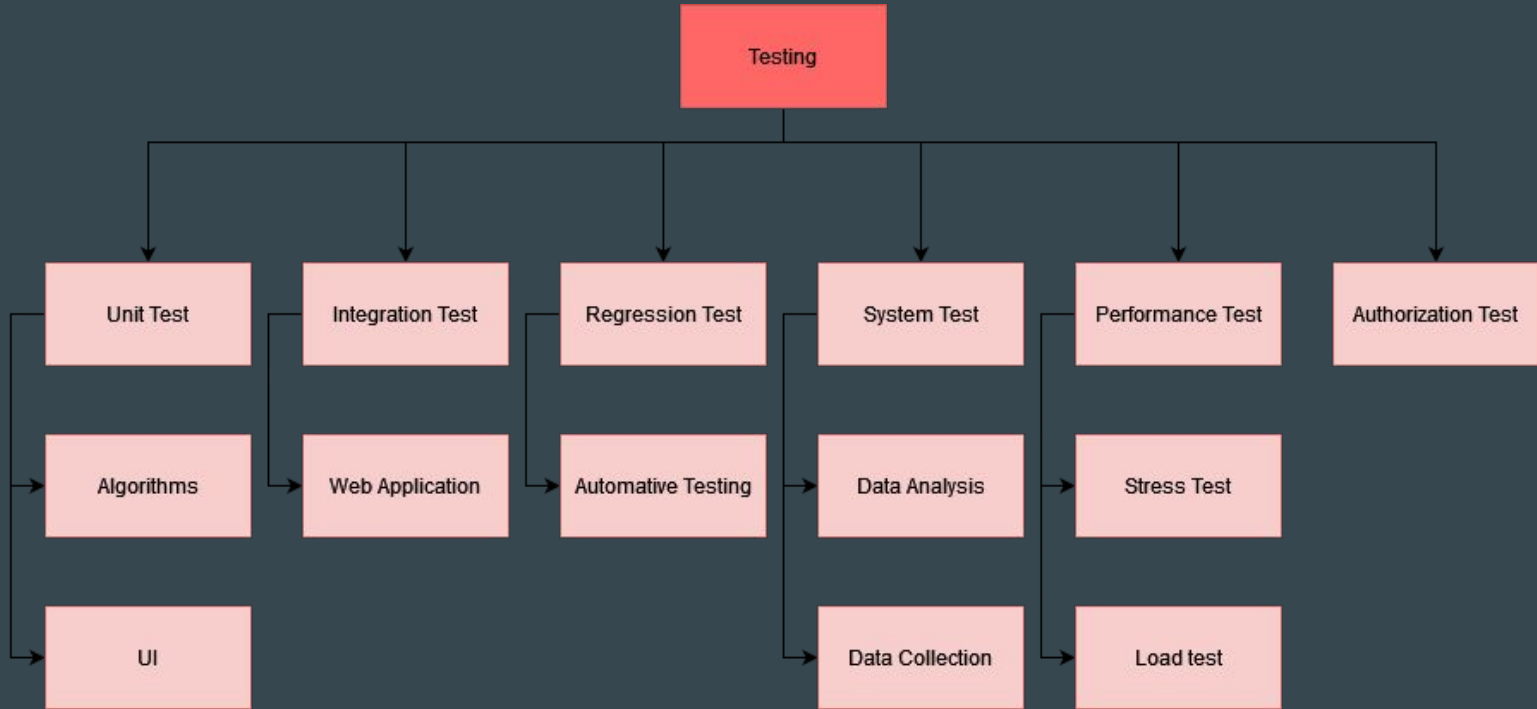
Prototype Major Functional Component Design



Software/Hardware Tools

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

Work Breakdown Structure - Testing



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 Account Management | Phishing Simulation | Feedback/Reports | User Interface | Sandboxed 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 effecting 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 Account Management | Phishing Simulation | Feedback/Reports | User Interface | Sandboxed 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 send fake phishing attacks to my students through Phisecure
- 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 Account Management | Phishing Simulation | Feedback/Reports | User Interface | Sandboxed 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 test connection to third person APIs.
- 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.
- As a tester, I need to generate “legitimate” emails

| User Account Management | Phishing Simulation | Feedback/Reports | User Interface | Sandboxed Phishing Environment | Analytics | Other |
|-------------------------|---------------------|------------------|----------------|--------------------------------|-----------|-------|
| | | | | | | |

Sprint Breakdown

Sprint 0 (Weeks 1-3)

- Establish development environment
- Setup front and back end infrastructure
- Develop UI framework
- Design database schema
- Design basic layouts for user registration and login screens
- Establish fake email environment
- Establish a baseline to implement Unit, System, and Integration testing procedures. These will be elaborated on in each sprint.

Sprint 3 (Weeks 12-14)

- Implement role-based access control
- Fine tune phishing campaign features
- Implement click rate tracking for phishing links
- Refine UI
- Update and implement new Unit, System, and Integration tests
- Implement regression testing procedures
- Implement performance testing procedures

Sprint 1 (Weeks 4-7)

- Develop the phishing campaign features
- Implement basic admin, student, and teacher dashboard
- Implement homepage layout
- Network layer analysis
- Update and implement new Unit, System, and Integration tests
- Implement regression testing procedures

Sprint 4 (Weeks 15-16)

- Add features for managing user accounts, permissions and campaigns
- Implement advanced analytics and reporting functionality
- Ensure readiness for production deployment
- Setup deployment configurations
- Update and implement new Unit, System, and Integration tests

Sprint 2 (Weeks 8-11)

- Implement phishing campaign features
- Implement dashboard statistics/performance metrics
- Set up email simulation
- Configure customizable network configurations
- Update and implement new Unit, System, and Integration tests

Technical Risk Matrix

| Risk Matrix | | Impact | | | | |
|-------------|----------------|---------------|-------|----------|-------|--------|
| | | Insignificant | Minor | Moderate | Major | Severe |
| Likelihood | Almost Certain | | | T3 | | |
| | Likely | | T3M | | | |
| | Possible | | | T1 | | |
| | Unlikely | | T1M | | T2M | |
| | 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. 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

| Risk Matrix | | Impact | | | | |
|-------------|----------------|---------------|-------|----------|------------|----------|
| | | Insignificant | Minor | Moderate | Major | Severe |
| Likelihood | Almost Certain | | | | | |
| | Likely | | | | C3 | C1 C2 |
| | Possible | | | | | |
| | Unlikely | | | C3M | C1M C2M | |
| | 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. 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

| Risk Matrix | | Impact | | | | |
|-------------|----------------|---------------|-------|----------|-------|--------|
| | | Insignificant | Minor | Moderate | Major | Severe |
| Likelihood | Almost Certain | | | | | |
| | Likely | | L2 | | L1 | |
| | Possible | | | L1M | | |
| | Unlikely | L2M | | | | |
| | 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.
- 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 \(cloudian.com\)](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, [ironsscales.com/blog/how-much-does-phishing-cost-businesses](https://www.ironsscales.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/](http://www.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-cybercams-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.