PHISECURE

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

17-22. The Solution

23. Major Functional Component Design

24-26. Phisecure: Its uses and its Users

27-29. Competition Comparison

30-32. Risk Matrix

33. 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.

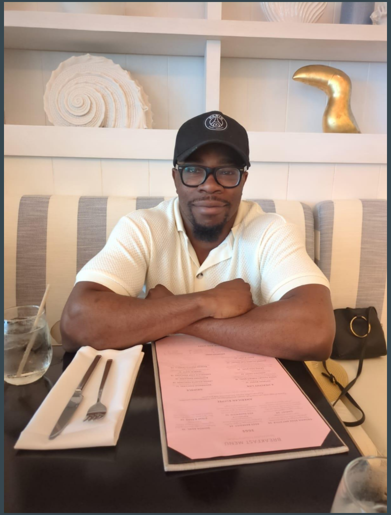
PHISECURE

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.

Problem Statement

Small businesses do not have the resources available to properly teach their employees to identify and avoid phishing attacks.

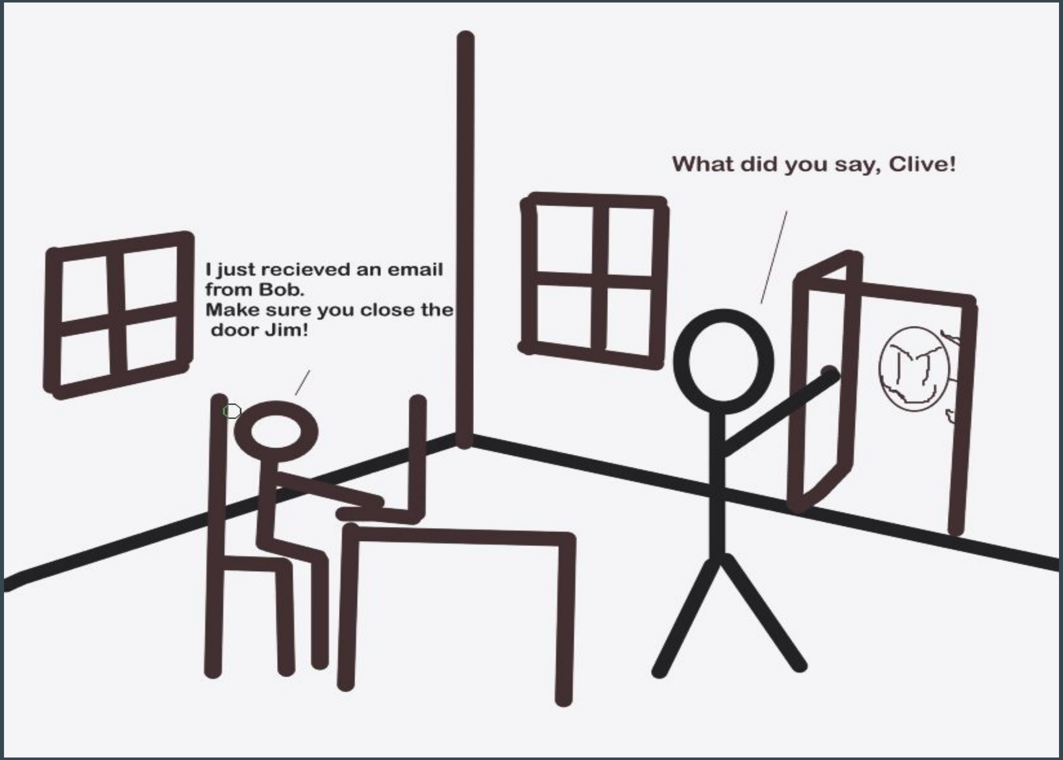
Phishing

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.[13]

Phishing

- Companies must maintain an internet presence to be successful.
    - In an article by Forbes that cites a Salesforce survey, “85% of consumers conduct research before they make a purchase online, and among the most used channels for research are websites (74%) and social media (38%)”.[14] Businesses rely more and more on the internet to grow and thrive.
- The web presence needed for growth makes companies vulnerable to phishing .
- To prevent phishing, companies must take action to acquire resources and knowhow to prevent, mitigate, and recover from phishing attacks.

Mo’ Phishing, Mo’ Problems

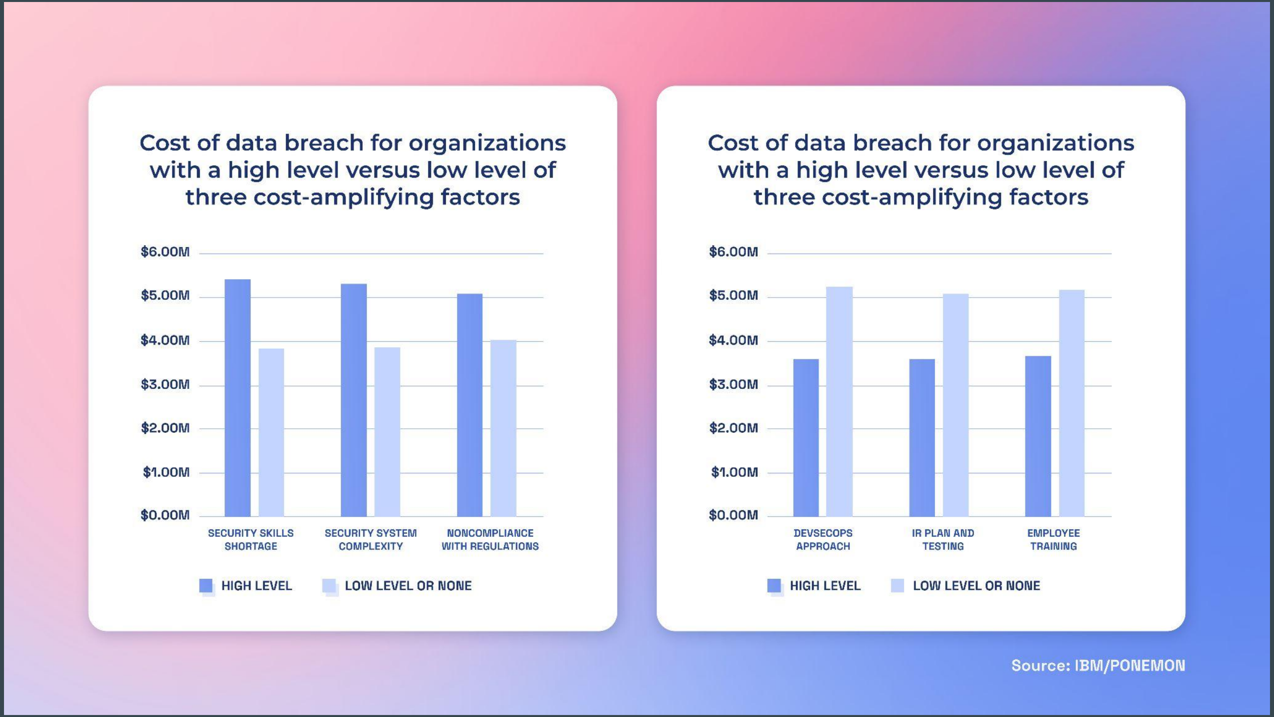


Mo’ Phishing, Mo’ Problems

Phishing *can and does* cost companies major money

- In a report by IronScales made in 2022, the average cost of a successful phishing attack was reported in the **4.5-5 million dollar range!**[5]
- A report by Egress stated “**Over half** (**58%**) [of surveyed organizations] had to cease operations while incidents were investigated, impacting organizational efficiency and the bottom line. In **49%** of organizations, client relationships were damaged from breached confidentiality, and just under one-quarter (**22%**) lost customers.”[6]

Cost of Data Breaches



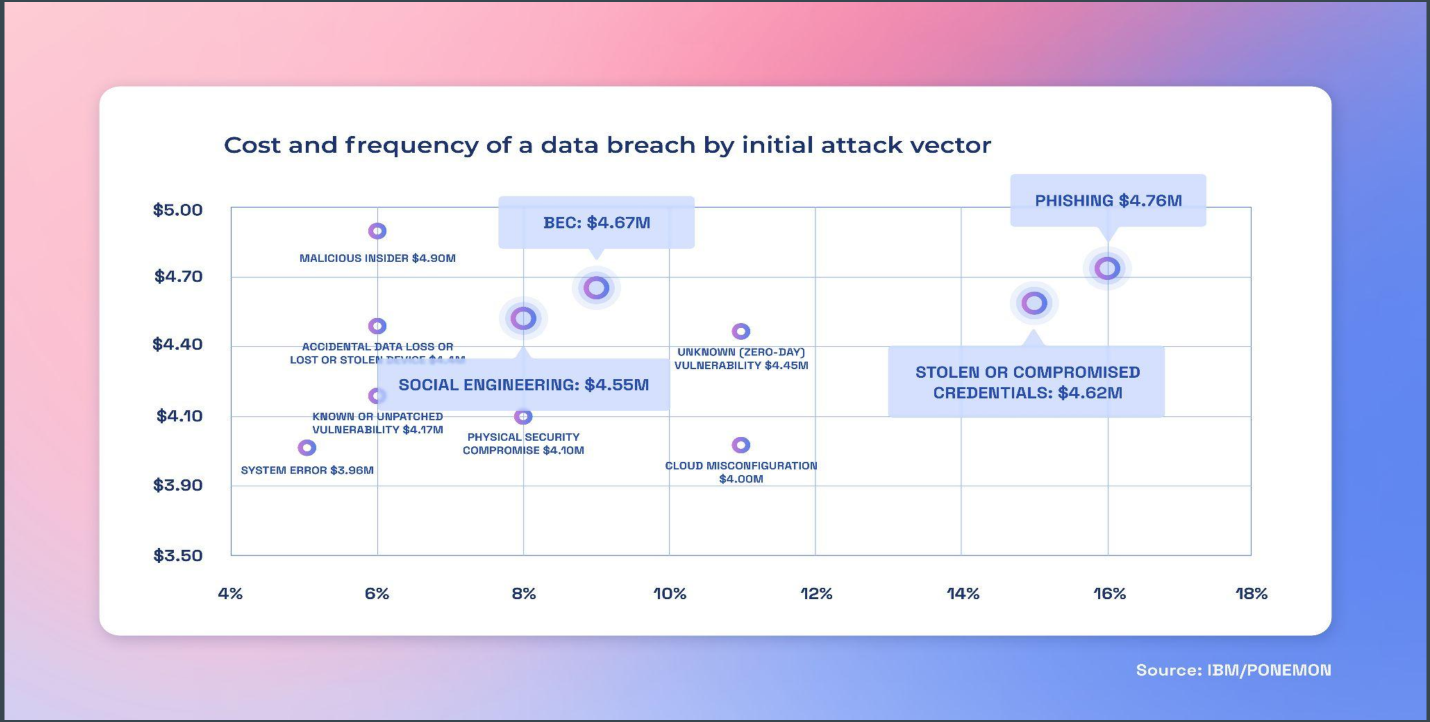
Cost of data breach for organizations with a high level versus low level of three cost-amplifying factors

Cost of data breach for organizations with a high level versus low level of three cost-amplifying factors

Source: IBM/PONEMON

2

Cost of Data Breaches



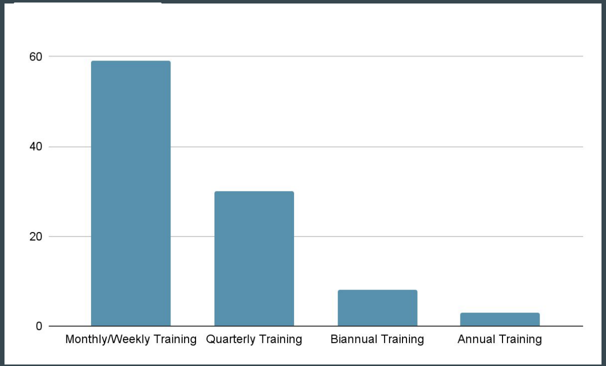
Cost and frequency of a data breach by initial attack vector

Source: IBM/PONEMON

Phishing Education

It's becoming increasingly clear that employees do NOT have the knowhow to successfully identify phishing scams.

- In a report by Egress whose statistics were aggregated by over 500 cybersecurity experts, **94%** of the organizations in the study were victims of a phishing attack![6]
  - In those cases, **74%** of the employees involved were disciplined in some way for their role in the attack!
- While companies *did* perform routine phishing training (statistics shown below), 74% of the training modules were either out-of-the-box solutions or standardized programs.
- It's clear that current iterations of phishing training are not specialized for the departments they are conducted in nor in-depth enough to be helpful. **We need something better**.



Problem Characteristics

- **Digital Dependency**: Dependence on technology in the digital age leaves small businesses exposed to more cyber threats.
- **Phishing Surge:** Phishing remains one of the top social engineering techniques that cyber criminals use to stage attacks.
- **Skill Gap**: While there is a growing demand for experts in the field there is a shortage of skilled cybersecurity professionals.
- **Limited Budget:** Small businesses do not have the budget to conduct security initiatives, including employee training on phishing awareness.
- **Lack of Time:** Rapid changes in the digital landscape often contributes to lack of time and resources for organizations to prioritize continual training.

Day In The Life

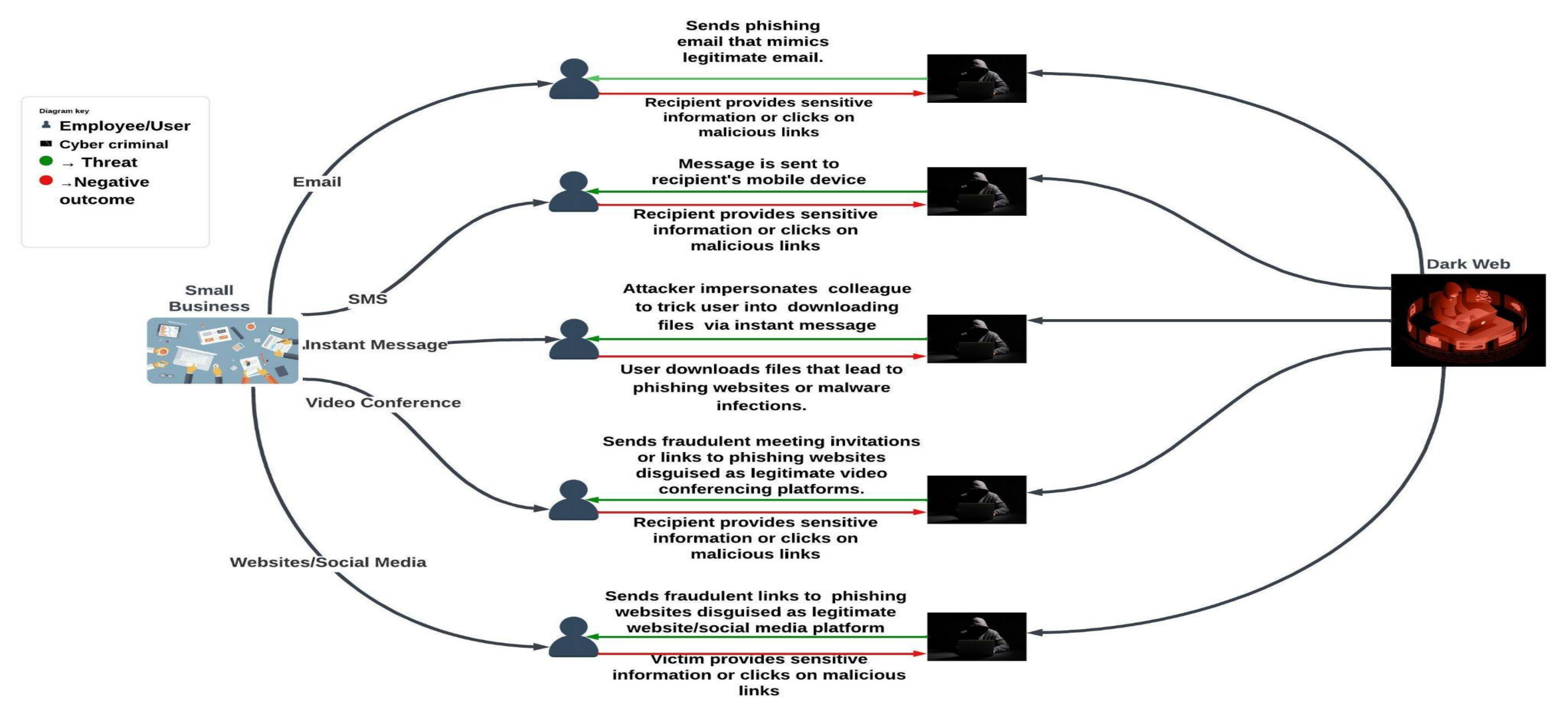


Diagram key

- Employee/User
- Cyber criminal
- ● → Threat
- ● → Negative outcome

Small Business

Email

SMS

Instant Message

Video Conference

Websites/Social Media

Dark Web

Sends phishing email that mimics legitimate email.

Recipient provides sensitive information or clicks on malicious links

Message is sent to recipient's mobile device

Recipient provides sensitive information or clicks on malicious links

Attacker impersonates colleague to trick user into downloading files via instant message

User downloads files that lead to phishing websites or malware infections.

Sends fraudulent meeting invitations or links to phishing websites disguised as legitimate video conferencing platforms.

Recipient provides sensitive information or clicks on malicious links

Sends fraudulent links to phishing websites disguised as legitimate website/social media platform

Victim provides sensitive information or clicks on malicious links

Current Process Flow

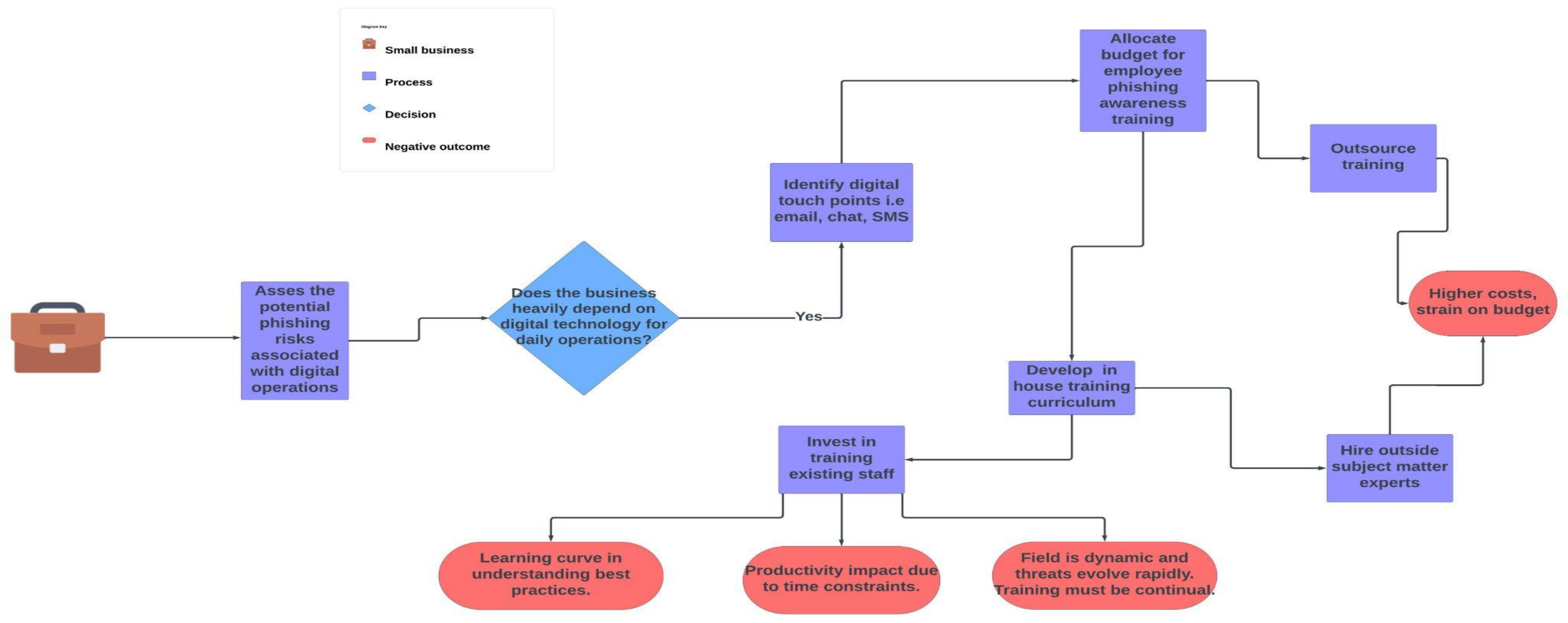


Diagram key

Small business

Process

Decision

Negative outcome

Asses the potential phishing risks associated with digital operations

Does the business heavily depend on digital technology for daily operations?

Yes

Identify digital touch points i.e email, chat, SMS

Allocate budget for employee phishing awareness training

Outsource training

Higher costs, strain on budget

Develop in house training curriculum

Hire outside subject matter experts

Invest in training existing staff

Learning curve in understanding best practices.

Productivity impact due to time constraints.

Field is dynamic and threats evolve rapidly. Training must be continual.

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 training process to help them identify phishing threats.

Solution Characteristics

Phishing Simulation

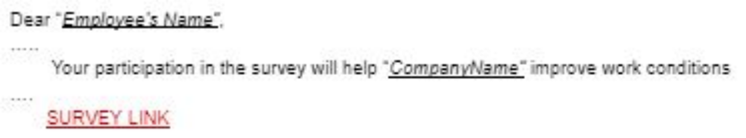
- Inputs given by the user will be used to generate unique phishing attacks.
- Sends messages through Email, Text, and Chat APIs used by workplaces or for personal use.

Provide feedback recorded from the simulation

- Reports to the user if they succeeded or failed the simulated phishing attack.
- Elaborates on the phishing methods used against them, demonstrating the red flags they should have noticed.

Simulation

- The templates will be generated and designed via Machine Learning



Dear "Employee's Name",

.....

Your participation in the survey will help "CompanyName" improve work conditions

....

SURVEY LINK

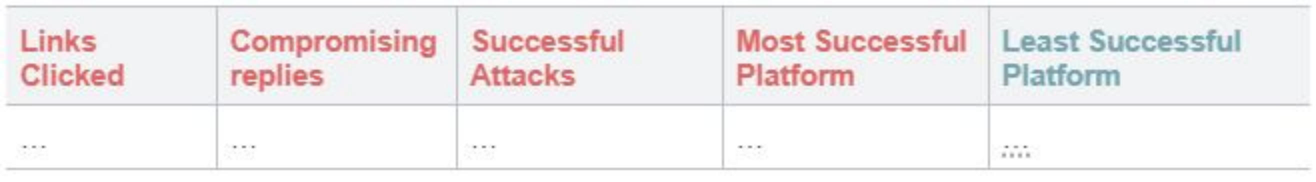
- Attack variation is important, email is not the only vulnerability

- 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.

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 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
...	...	...	...	...

Solution Process Flow

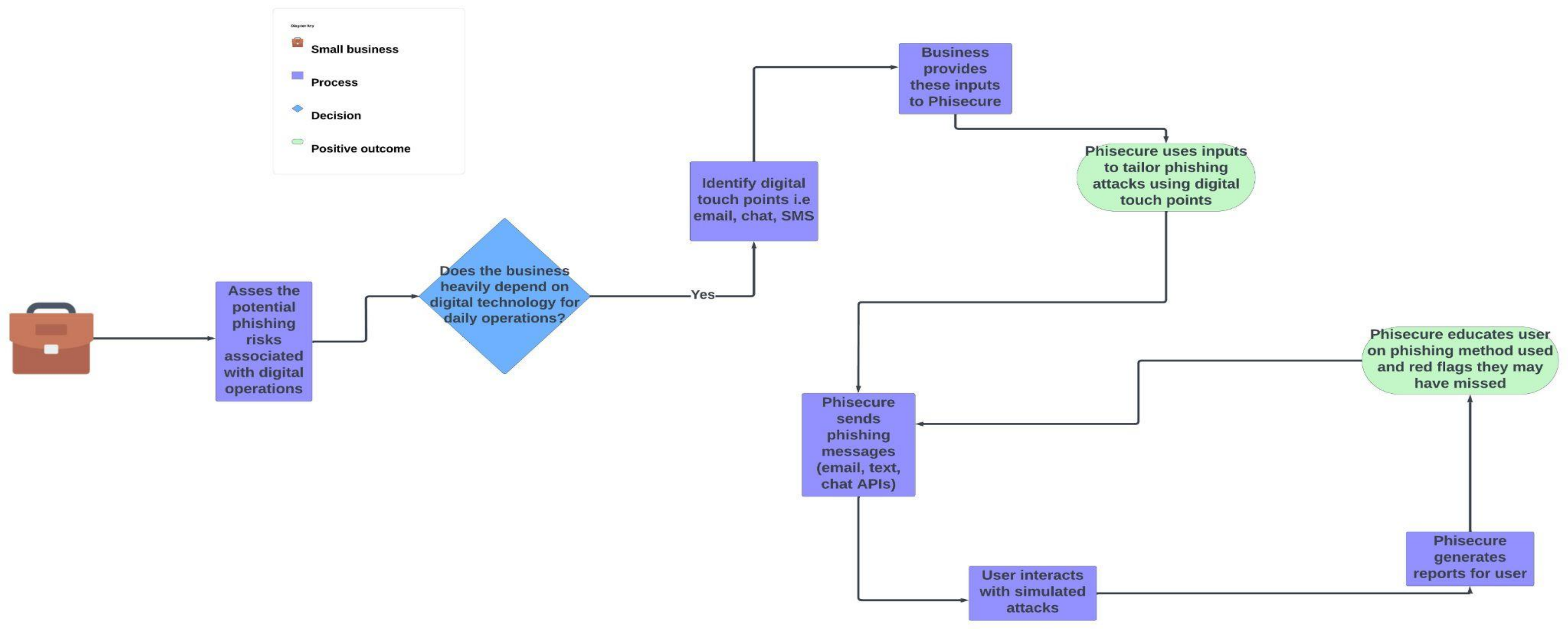


Diagram key

Small business

Process

Decision

Positive outcome

Asses the potential phishing risks associated with digital operations

Does the business heavily depend on digital technology for daily operations?

Yes

Identify digital touch points i.e email, chat, SMS

Business provides these inputs to Phisecure

Phisecure uses inputs to tailor phishing attacks using digital touch points

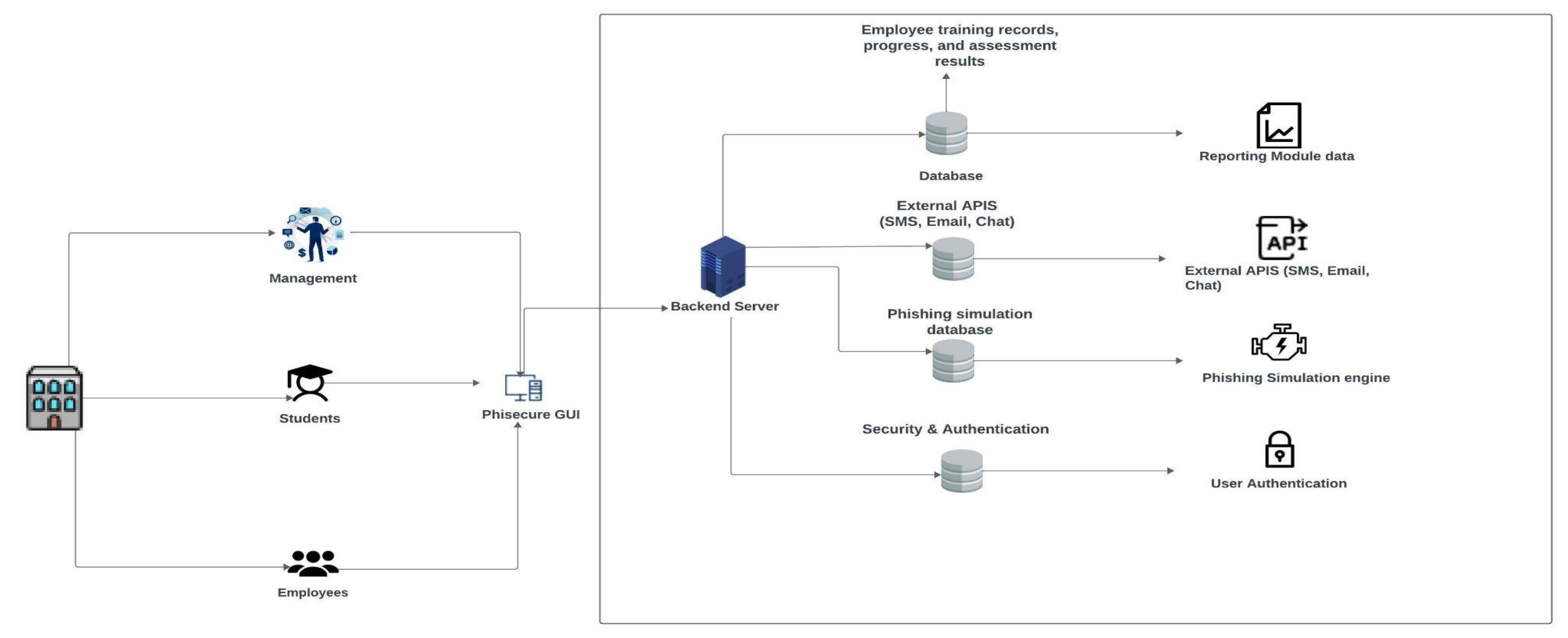
Phisecure sends phishing messages (email, text, chat APIs)

User interacts with simulated attacks

Phisecure generates reports for user

Phisecure educates user on phishing method used and red flags they may have missed

Major Functional Component Design


Employee training records, progress, and assessment results
Database
Reporting Module data
Management
External APIS (SMS, Email, Chat)
API
External APIS (SMS, Email, Chat)
Backend Server
Phishing simulation database
Phishing Simulation engine
Students
Phisecure GUI
Security & Authentication
User Authentication
Employees

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:

- Small businesses
- Universities

End-Users:

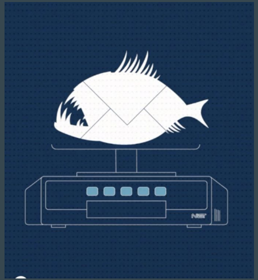
- Employees
- Students

Stakeholders:

- Organization Leadership (Executives, CEO, CISO, Dean)
- Regulatory Authorities
- Human Resources

		Direct Competition			Indirect Competition	
	PHISECURE	KnowBe4	HoxHunt	Infosec IQ	Universities	Nice Challenge Project
Affordable <$1 per person	✓	□	□	□	✅	✅
SMS and Other Business Software Impersonated	✓	✅	□	□	□	✅
Simulation of Phishing Attacks	✓	✅	✅	✅	□	□
Designed for the Average User	✓	✅	✅	✅	✅	□
Templates based on the National Institute of Standards and Technology's Phish Scale	✓	□	□	□	□	✅
Peer Driven Spear Phishing	✓	□	□	□	□	□
Peer Training Effectiveness Assessment	✓	✅	✅	✅	✅	✅

Phish Scale



Cues [2]

- Indicators
  - Errors
  - Technical
  - Visual
- Hooks
  - Language & Content
  - Common Tactics

Premise Alignment Method One[2]

- Levels
  - High
  - Medium
  - Low
- Whether the subject matter is appropriate for the target audience

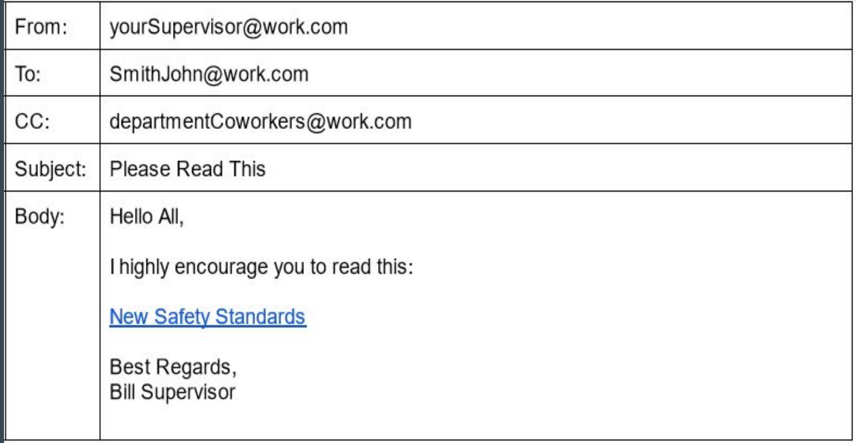
Premise Alignment Method Two[2]

- Formulaic Approach on a five-point scale
- Criteria
  - Mimics a workplace process or practice
  - Has workplace relevance
  - Aligns with other situations or events, including external to the workplace
  - Engenders concern over consequences for NOT clicking
  - Has been the subject of targeted training, specific warnings, or other exposure

Examples

Very Difficult: Link Attack

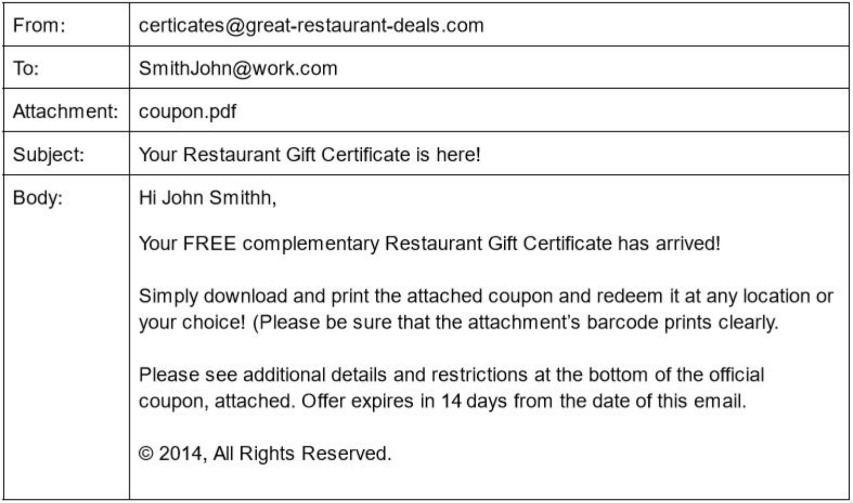
- Number of Cues: Few
- Premise Alignment Method One: High
- Premise Alignment Method Two: High



From:	yourSupervisor@work.com
To:	SmithJohn@work.com
CC:	departmentCoworkers@work.com
Subject:	Please Read This
Body:	Hello All, I highly encourage you to read this: New Safety Standards Best Regards, Bill Supervisor

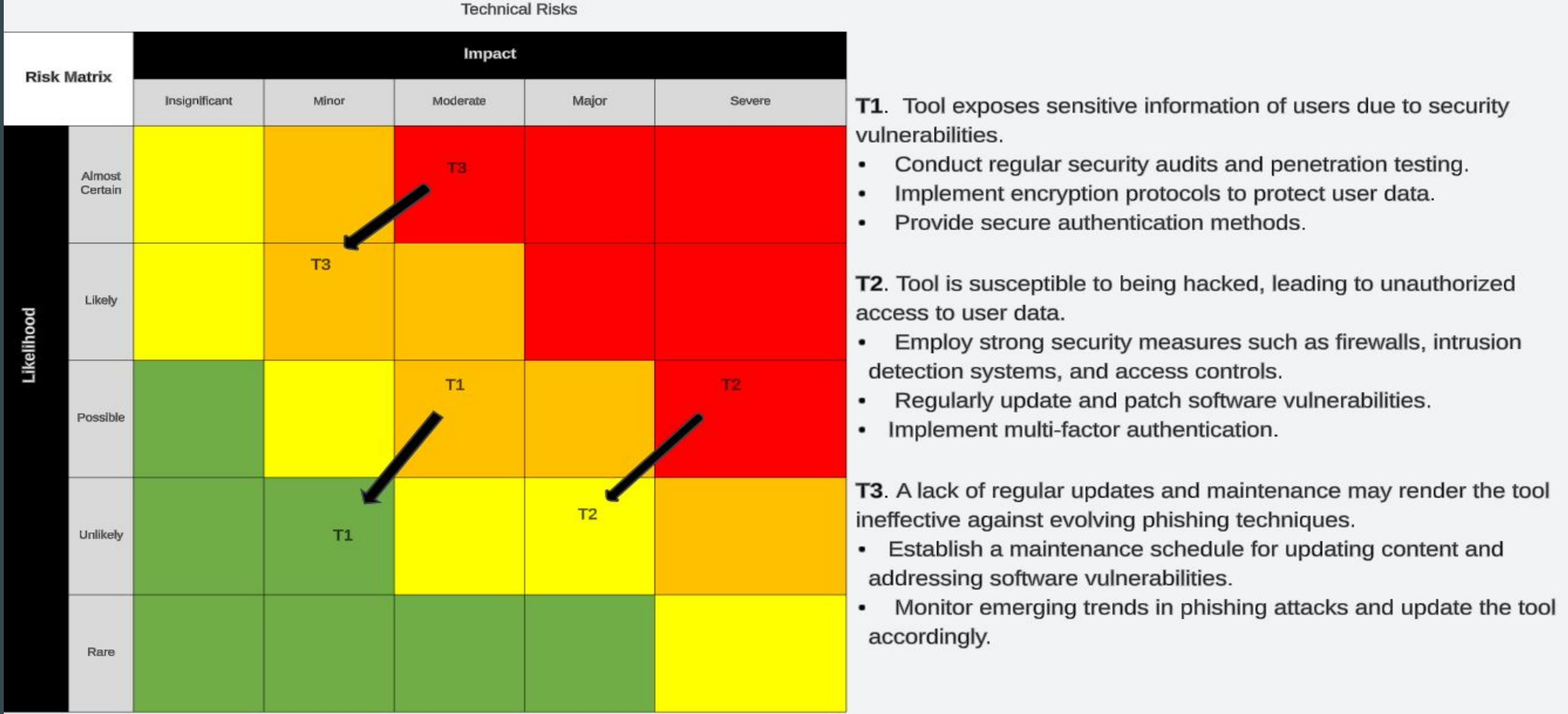
Moderately/Least Difficult: Attachment Attack[2]

- Number of Cues: Some
- Method One: Low
- Method Two: Low



From:	certicates@great-restaurant-deals.com
To:	SmithJohn@work.com
Attachment:	coupon.pdf
Subject:	Your Restaurant Gift Certificate is here!
Body:	Hi John Smithh, Your FREE complementary Restaurant Gift Certificate has arrived! Simply download and print the attached coupon and redeem it at any location or your choice! (Please be sure that the attachment's barcode prints clearly. Please see additional details and restrictions at the bottom of the official coupon, attached. Offer expires in 14 days from the date of this email. © 2014, All Rights Reserved.

Technical Risk Matrix



Technical Risks

Risk Matrix		Impact				
		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.

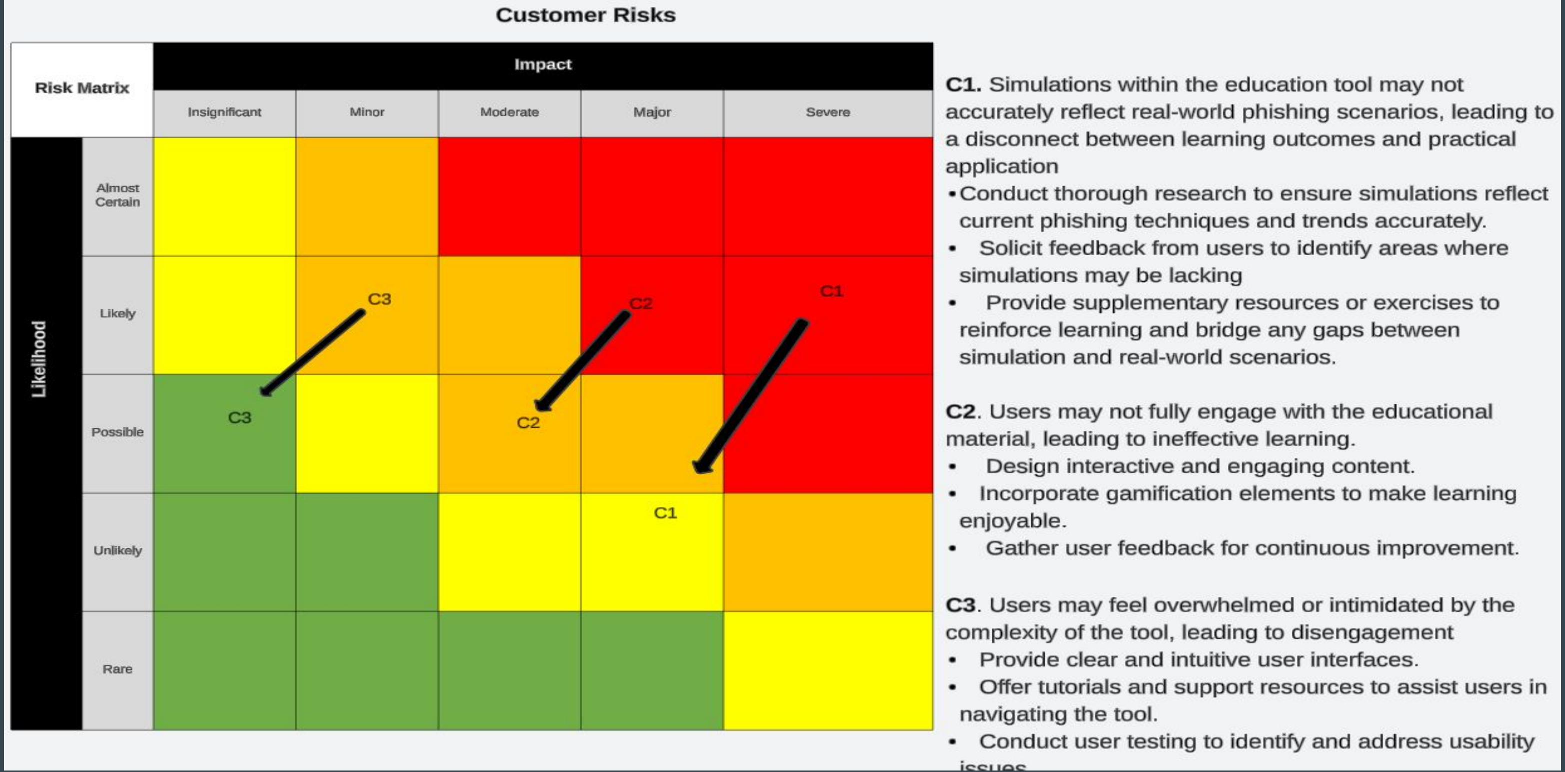
T2. Tool is susceptible to being hacked, leading to unauthorized access to user data.

- 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.

Customer Risk Matrix



Customer Risks

Risk Matrix		Impact				
		Insignificant	Minor	Moderate	Major	Severe
Likelihood	Almost Certain	🟨	🟧	🟥	🟥	🟥
	Likely	🟨	🟧 C3	🟧	🟥 C2	🟥 C1
	Possible	🟩 C3	🟨	🟧 C2	🟧	🟥
	Unlikely	🟩	🟩	🟨	🟨 C1	🟧
	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.
- Solicit feedback from users to identify areas where simulations may be lacking
- Provide supplementary resources or exercises to reinforce learning and bridge any gaps between simulation and real-world scenarios.

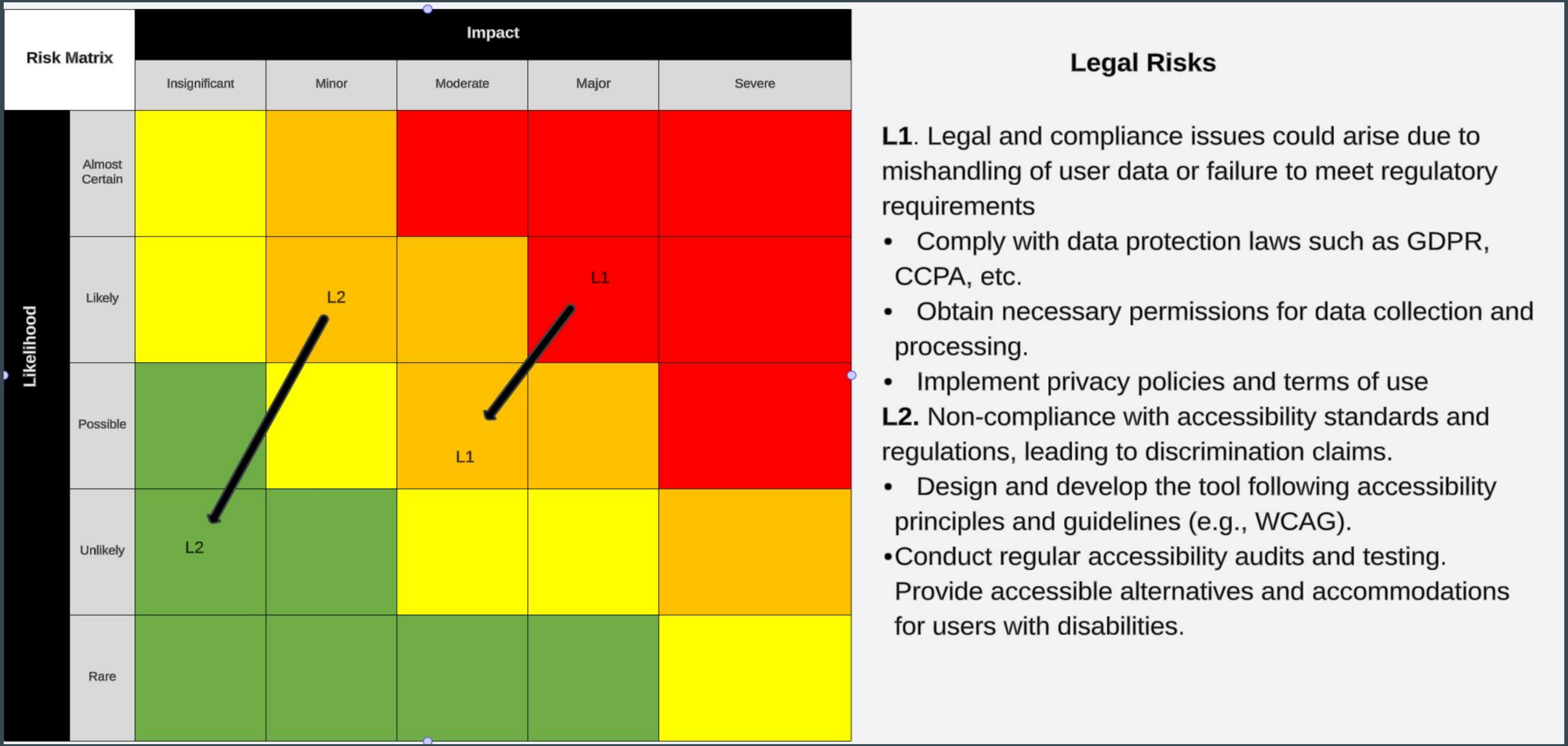
C2. Users may not fully engage with the educational material, leading to ineffective learning.

- 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

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 businesses
- Phisecure offers a tailored solution, which provides customizable phishing simulations.
- Through collaboration with universities, Phisecure enhances its reach, offering innovative cybersecurity education to businesses.

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.

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.