

# DeepPhish Simulation + Risk Assessment Report

Assessment Date: April 13, 2025

Report Generated: 2025-04-13 01:48:49

---

## 1. Risk Pre-Assessment

The following image provides additional context or data for this assessment:



Source: 3d\_risk\_surface.png

## 2. Executive Summary

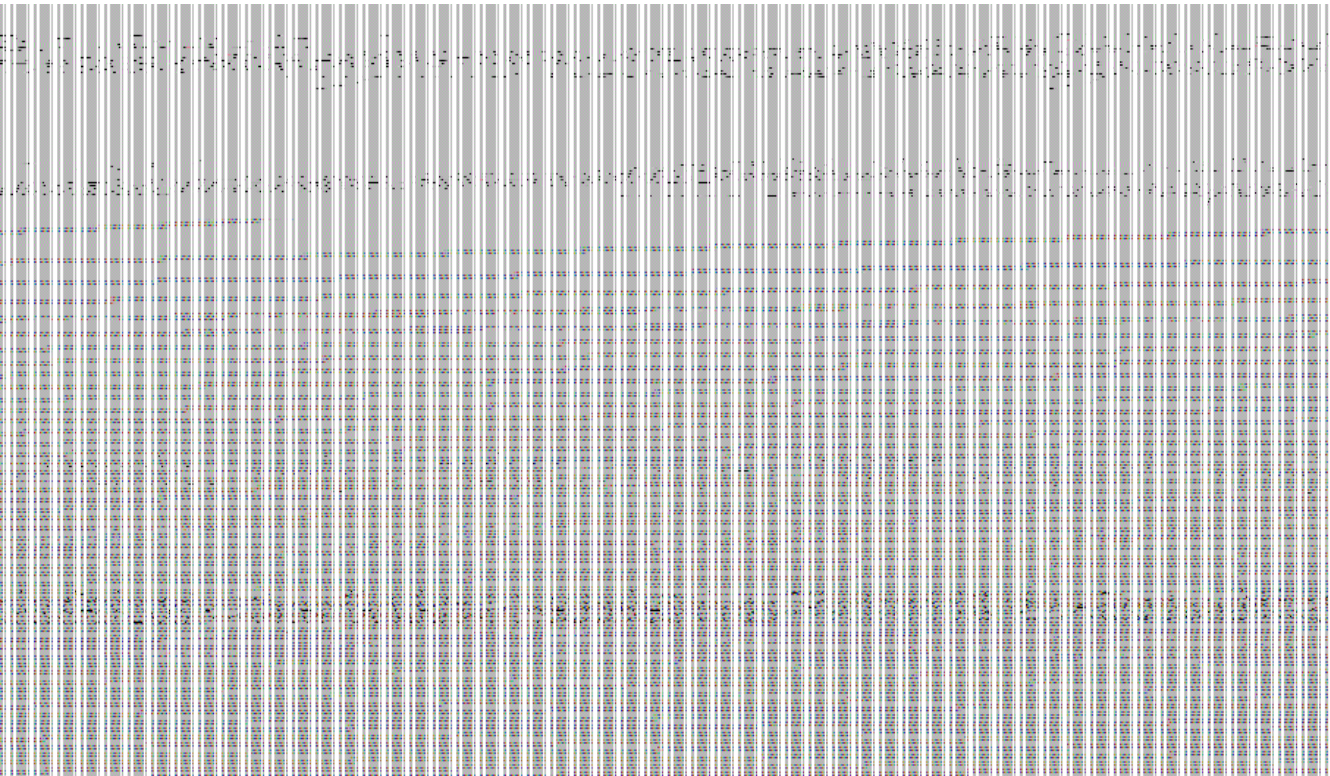
This report presents the results of a phishing simulation exercise conducted on April 13, 2025. A total of 12 employees were included in the test to evaluate their response to a simulated phishing threat.

- Clicked the link: 6 employees (50.0%)
- Reported the phish: 4 employees (33.3%)
- Ignored the email: 2 employees (16.7%)
- Remediation needed: 5 employees

This data highlights both areas of strength and potential risks within the organization's current awareness levels.

## 3. Simulation Response Visualization

Below is a graphical representation of employee responses during the simulation:



## 4. Detailed Interaction Log

The following table contains a log of all participants and their corresponding actions during the simulation.

Employee Name	Status	Department	Reported Date
Augusto	Clicked Link - Remediation Required	IT	2025-04-13
Matthew	Clicked Link - Remediation Required	Engineering	2025-04-13
Alice Smith	Clicked Link - Remediation Required	Sales	None
Bob Johnson	Reported Phish	Engineering	2025-04-10
Charlie Brown	Ignored	Marketing	None
Diana Prince	Clicked Link - Remediation Required	Sales	None
Ethan Hunt	Reported Phish	Engineering	2025-04-11
Fiona Glenanne	Reported Phish	Marketing	2025-04-10
George Constanza	Clicked Link - Remediation Complete	Sales	2025-04-12
Hannah Abbott	Ignored	Engineering	None
Ian Malcolm	Clicked Link - Remediation Required	Marketing	None
Jane Doe	Reported Phish	Sales	2025-04-11

## 5. Analysis & Strategic Recommendations

This phishing simulation provides meaningful insights into the organization's readiness against social engineering threats. Key findings and actionable recommendations are outlined below:

- **Targeted Remediation Training**  
Provide mandatory training to the 5 employees who interacted with the phishing email. Focus on spotting red flags, verifying sender legitimacy, and best practices for email handling.
- **Positive Reinforcement & Recognition**  
Acknowledge the 4 employees who correctly reported the phishing attempt. Recognition can increase motivation and awareness across the team.
- **Technical Control Audit**  
Review the effectiveness of current email filtering, anti-spoofing protocols (DMARC, DKIM, SPF), and threat detection systems to reduce phishing exposure.
- **Ongoing Testing**  
Plan the next simulation for Q3 2025. Iterative testing improves long-term resilience and tracks security awareness progress.

---

Report compiled by the DeepPhish for the ML@ Purdue Hackathon!