Phishing Awareness Simulation Report

1. Introduction

Phishing remains the most critical initial attack vector for cyber security breaches, consistently exploiting human vulnerability rather than relying on sophisticated technical flaws. This project aimed to move beyond theoretical knowledge by conducting an ethical, controlled phishing simulation in a secure, informed environment.

The primary objective was to measure the current level of user awareness against modern social engineering tactics, specifically focusing on urgent password reset requests. The goal was to identify critical gaps where security training could be most effective, transitioning users from being potential victims to becoming an active part of the organization's **"Human Firewall."** Adherence to cyber ethics, including obtaining informed consent from all participants and ensuring no real data was compromised, was maintained throughout the simulation.

2. Methodology

The simulation followed a structured, four-phase methodology mimicking an ethical hacking lifecycle: Research, Design, Execute, and Analyze.

3. Results

The simulation yielded the following quantitative results, illustrating the group's current vulnerability level against high-urgency attacks:

Metric	Count (N=50)	Percentage	Assessment
Emails Sent	50	100%	Baseline
Emails Opened	35	**70%**	High Engagement
Clicked Link (CTR)	12	**24%**	Significant Failure
Submitted Credentials (Compromised)	5	**10%**	Critical Risk

Analysis:

- **Critical Risk Level:** The **10% Compromise Rate** (5 users who submitted credentials) is slightly lower than some industry benchmarks but still represents a critical failure rate. In a real-world scenario, 10% of the organization would have been compromised, providing attackers with initial access to systems, data, or networks.

- **Need for Scrutiny:** The 24% click rate indicates a substantial lack of diligence in checking fundamental red flags like the sender's full email address before proceeding to the link.

4. Lessons Learned

The simulation provided valuable, action-oriented insights into specific areas of user weakness:

- **Failure to Verify Source:** The primary failure point was a lack of diligence in checking the sender's actual email address and the destination URL. Most successful victims admitted to focusing only on the display name and the urgent message body, overlooking suspicious details in the email header.
- **Subtle Errors are Missed:** While the fake login page had subtle inconsistencies (e.g., generic URL, slightly off-branding), these were ignored once the user was focused on the task of entering data.

5. Preventive Measures

To address the identified vulnerabilities and reduce the organization's overall **Phish-Prone Percentage (PPC)**, the following technical controls and awareness methods are strongly recommended.