Phishing Awareness Simulation Report

1. Introduction

Phishing remains the most critical initial attack vector for cyber security breaches, exploiting human vulnerability rather than technical flaws. This project aimed to move beyond theoretical knowledge by conducting an ethical, controlled phishing simulation. The primary objective was to measure the current level of user awareness against social engineering tactics, specifically focusing on urgent password reset requests, and to identify areas where security training could be most effective.

The simulation was executed in a controlled environment with **informed consent** from all participants, ensuring adherence to cyber ethics. The core goal was to transition users from being potential victims to becoming an active part of the organization's "Human Firewall."

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:

Metric	Count (N=50)	Percentage
Emails Sent	50	100%
Emails Opened	35	70%
Clicked Link (CTR)	12	24%
Submitted Credentials (Compromised)	5	10%

Analysis:

- **High Engagement:** The high open rate (70%) confirms the effectiveness of using "Urgency" and "Authority" in the email subject line.
- **Critical Risk Level:** The **10% Compromise Rate** (5 users who submitted credentials) is slightly lower than the documented industry average of approximately 17.8% but still represents a critical failure rate. In a real-world

scenario, 10% of users would have been compromised, providing attackers with initial access to the system.

4. Lessons Learned

The simulation provided valuable, action-oriented insights into user behavior:

- **Failure to Verify:** 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.
- **The Power of Urgency:** The use of phrases like "Action Required" and "Immediate Suspension" successfully bypassed critical thinking. Users prioritized quick compliance over security verification.
- **Subtle Errors are Missed:** While the fake login page had subtle inconsistencies (e.g., generic URL, slightly off-branding in the simulated Google Form), these were ignored once the user was focused on entering data.
- **Reporting Mechanism Weakness:** No users initially reported the email as suspicious; they either engaged with it or deleted it. This highlights a gap in the organizational defense mechanism, as early reporting is vital for mitigating attacks.

5. Preventive Measures

To address the identified vulnerabilities and reduce the organization's overall phish-prone percentage, the following countermeasures and awareness methods are recommended:

A. Technical Controls

1. **Mandatory Multi-Factor Authentication (MFA):** This is the single most effective countermeasure. Even if a user's password is stolen, the attacker cannot log in without the second factor (e.g., a code from a mobile app).
2. **Advanced Email Filtering:** Implement or tune filters to scan for domain spoofing, suspicious links, and high-risk keywords (e.g., "urgent," "payment," "reset").

B. Awareness and Training

1. **Continuous Simulation Training:** Regular, unannounced phishing simulations should be conducted monthly. Training should immediately follow a failed attempt, focusing specifically on the red flags missed by the individual.
2. **"Hover & Inspect" Principle:** Train users to habitually hover their cursor over links to inspect the destination URL before clicking. If the URL is unfamiliar, a link

shortener, or does not match the expected domain (e.g., not microsoft.com or google.com), they must not proceed.

3. **Establish a Clear Reporting Channel:** Implement an easily accessible "Report Phishing" button in the email client. All employees must be trained that reporting a suspected phishing email is a non-punitive, high-priority action.
4. **Verification Protocol:** Promote a zero-trust mindset for urgent IT requests. Users should be instructed to independently verify all password change or security alert requests by logging in directly to the official platform (e.g., going to outlook.com directly) or by calling the known IT helpdesk number.