Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 11

Phishing Simulation Report

This report presents a comprehensive phishing simulation designed to evaluate and improve organizational security awareness. It follows eight defined steps and serves both as a technical reference and an educational resource for employees and security teams.

Understanding Phishing Attacks

Phishing is a form of social engineering where attackers impersonate trusted entities to steal sensitive information.

Modern phishing techniques (2026):

- **Spear Phishing**
  Highly targeted attacks crafted for specific individuals.
- **Business Email Compromise (BEC)**
  Attackers impersonate executives to trick employees into approving payments or sharing data.
- **Quishing**
  Malicious QR codes used to bypass traditional email security controls.

Psychological tactics used:

- Urgency
- Authority
- Fear

These triggers push victims to act quickly without verifying authenticity.

Fake Email Template Creation

A realistic email lure is critical for an effective simulation. The following template mimics a corporate security alert.

Field	Content
Subject	Urgent: Security Update Required for {{.Email}}
Sender	IT Security Support <support@corp-security-portal.com>
Body (HTML)	Dear {{.FirstName}}, Our systems detected an unauthorized login attempt on your account. To prevent unauthorized access, please verify your identity immediately. Verify My Account Now Failure to verify within 12 hours will result in account suspension.

Landing Page Setup

The landing page acts as the credential capture point in the simulation.

Key components:

- **Cloning:**
  A cloned version of the internal corporate login portal is used.
- **Fields:**
  Username and password input fields.
- **Data Handling:**
  GoPhish records the event as “Data Submitted” without storing plaintext passwords.
- **Redirection:**
  After submission, users are redirected to a *Teachable Moment* page explaining the simulation.

Sending the Test Phishing Email

Execution steps:

- **SMTP Configuration:**
  A sending profile is created in GoPhish using a dedicated mail server.
- **Targeting:**
  Users and groups are imported into the campaign.
- **Launch:**
  The campaign is scheduled and sent.
  GoPhish generates a unique tracking URL for each recipient.

Tracking User Responses

User interactions are monitored in real time using the GoPhish dashboard.

Tracked metrics:

1. **Sent** – Email successfully sent from the server
2. **Opened** – Detected via a hidden 1×1 transparent tracking pixel
3. **Clicked** – User clicks the unique phishing URL
4. **Submitted Data** – User enters credentials on the landing page

---

Identifying Phishing Red Flags

Employees are trained to recognize common warning signs:

- **Mismatched Domain**
  @corp-security-portal.com instead of the official @company.com
- **Artificial Urgency**
  Threat of account suspension within 12 hours
- **Suspicious Links**
  Hovering over links reveals unfamiliar URLs
- **Generic Greetings**
  Many phishing emails use “Dear Employee” instead of real names

---

Prevention and Mitigation Strategies

To reduce real-world phishing success, organizations should implement:

- **Multi-Factor Authentication (MFA)**
  Prevents account compromise even if credentials are stolen
- **Email Authentication**
  DMARC, SPF, and DKIM to stop domain spoofing
- **Clear Reporting Process**
  “Report Phish” button for rapid security team response
- **Continuous Education**
  Regular, non-punitive simulations to build long-term awareness

---

Simulation Documentation

This document serves as the official record of the phishing simulation.

Key details:

- **Objective:**
  Measure and improve resilience against social engineering
- **Scope:**
  Employees included in the designated test group
- **Outcome:**
  Results identify high-risk areas and guide future training
- **Conclusion:**
  Phishing is a human-centric threat that requires a human-centric solution: awareness