Comprehensive Social Engineering Campaign Plan

# Objective

To evaluate and enhance employees' awareness and handling of social engineering attacks through phishing emails, phone calls (vishing), and physical methods like dropping USB drives.

# Tools

• GoPhish: A phishing simulation tool to create and manage phishing campaigns.

• SET (Social-Engineer Toolkit): A suite of tools designed for various social engineering attacks, including email phishing and vishing.

# Phishing Campaign

## 1. Research and Design

Objective: Create phishing emails that mimic common legitimate communications to assess employee susceptibility.

Approach: Identify common legitimate emails such as HR announcements, IT support notifications, and corporate communications. Analyze their structure, language, and design to replicate them accurately.

Example Scenarios:

* • HR Announcements: Emails about new company policies, benefits updates, or mandatory training.
* • IT Support: Password reset requests, security updates, or account verification emails.

## 2. Phishing Simulation Tool

Tool: Utilize a phishing simulation tool like GoPhish to automate the distribution and tracking of phishing emails.

Setup: Configure the tool with the designed email templates and target employee groups. Schedule the email dispatch for optimal testing times.

## 3. Monitoring and Data Collection

Metrics: Track key metrics such as email open rates, click-through rates, and information submission rates.

Data Collection: Gather detailed data on employee interactions with the phishing emails to identify patterns and vulnerabilities.

## 4. Effectiveness Evaluation

Scenario Analysis: Compare the effectiveness of different phishing scenarios to determine which types of emails are more likely to deceive employees.

Target Group Analysis: Assess the susceptibility of different employee groups (e.g., by department, seniority) to identify high-risk areas.

## 5. Reporting

Findings: Prepare a comprehensive report detailing the campaign's findings, including statistical data and patterns observed.

Recommendations: Provide actionable recommendations for improving email security awareness and reducing susceptibility to phishing attacks. Suggest targeted training programs and policy updates.

# Vishing Campaign

## 1. Script Development

Objective: Create convincing vishing scripts to test employees' response to phone-based social engineering attacks.

Approach: Tailor scripts to different scenarios such as IT suft5et5 fer4 swtpport calls, customer service inquiries, or urgent security alerts.

Example Scenarios:

* • IT Support: Calls requesting verification of login details due to a suspected breach.
* • Customer Service: Calls seeking personal information for account verification or troubleshooting.

## 2. Ethical and Legal Compliance

Guidelines: Ensure all vishing activities comply with ethical guidelines and legal regulations. Obtain necessary approvals and inform relevant stakeholders about the campaign.

Privacy: Maintain employee privacy and confidentiality throughout the process.

## 3. Conducting Vishing Calls

Execution: Perform vishing calls using the developed scripts. Ensure a realistic and convincing delivery to effectively test employees' responses.

Outcome Recording: Document the outcomes of each call, noting instances of successful information extraction, employee denial, or suspicion.

## 4. Effectiveness Analysis

Script Evaluation: Analyze the effectiveness of different vishing scripts to identify which scenarios are more likely to succeed.

Responsiveness Analysis: Assess the responsiveness of different employee groups to identify high-risk areas and potential weaknesses.

## 5. Reporting

Findings: Compile a detailed report on the vishing campaign's findings, including call outcomes and patterns observed.

Recommendations: Provide recommendations for enhancing phone security practices, such as implementing stricter verification procedures and conducting regular awareness training.

# USB Drop Campaign

## 1. Preparation

Objective: Test employees' reactions to finding and using suspicious USB drives.

Approach: Prepare USB drives with harmless files labeled as sensitive information (e.g., "Confidential\_Salary\_Report.pdf").

Labeling: Ensure USB drives are convincingly labeled to entice curiosity.

## 2. Deployment

Location: Strategically place USB drives in common areas (e.g., parking lots, restrooms, break rooms).

Monitoring: Track which drives are picked up and connected to the network.

## 3. Data Collection

Metrics: Monitor the number of USB drives picked up and connected to employee computers.

Analysis: Evaluate the potential security risk posed by employees connecting unknown USB drives to their workstations.

## 4. Reporting

Findings: Document the results, including the number of USB drives picked up and used.

Recommendations: Suggest improvements to physical security awareness, such as not using unknown USB drives and reporting suspicious devices.

# Comprehensive Reporting and Recommendations

## 1. Consolidated Report

Data Analysis: Integrate findings from phishing, vishing, and USB drop campaigns into a single comprehensive report.

Statistics: Include detailed statistics on response rates, success rates, and identified vulnerabilities.

Patterns: Highlight patterns and trends observed across different employee groups and scenarios.

## 2. Actionable Recommendations

Training Programs: Develop targeted training programs based on identified weaknesses.

Policy Updates: Suggest updates to security policies and procedures to address the vulnerabilities discovered.

Continuous Improvement: Recommend regular social engineering testing and training to maintain high levels of security awareness.

# Figures and Tables to put

• Figure 1: Example Phishing Email Template.

• Figure 2: Example Vishing Call Script.

• Table 1: Phishing Campaign Response Rates.

• Table 2: Vishing Call Outcomes.

• Table 3: USB Drop Success Rates.