**Social Engineering Awareness Campaign Plan**

**Page 1: Understanding Social Engineering Techniques**

Social engineering is a manipulation technique used by cybercriminals to trick individuals into giving away confidential information. Below are four common social engineering tactics, their red flags, and examples from recent breaches:

1. **Phishing**
   * **Definition**: Sending fraudulent messages that appear to come from a trusted source, typically via email.**Red Flags**: Urgent language, suspicious links, grammatical errors, unfamiliar senders.
   * **Example**: In 2020, Twitter suffered a major breach where attackers used spear-phishing to access internal systems, leading to the takeover of high-profile accounts.
2. **Pretexting**
   * **Definition**: Creating a fabricated scenario to trick the target into revealing personal information.**Red Flags**: Unusual or excessive requests for sensitive data, impersonation of authority figures.
   * **Example**: In the Sony Pictures hack (2014), attackers posed as company IT staff to extract login credentials from employees.
3. **Baiting**
   * **Definition**: Offering something enticing (e.g., free software or USB drives) to lure victims into compromising security.**Red Flags**: Offers too good to be true, unsolicited giveaways.
   * **Example**: A 2018 study found that nearly half of dropped USBs were plugged into enterprise machines, leading to malware infections.
4. **Tailgating (Piggybacking)**
   * **Definition**: Gaining physical access by following an authorized person into a restricted area.**Red Flags**: Unknown individuals asking to be let in, "forgot my badge" excuses.
   * **Example**: In multiple penetration tests, attackers gained access simply by walking behind employees through secure doors.

****

**Asset 2: Mock Phishing Email (Training Test)**

*Subject: Important: Password Expiry Notification*

*Body:* "Your password is set to expire in 24 hours. To maintain access, please update your credentials immediately by clicking the link below:

[Reset Password Now]"

*Sender:* ITSupport@organization-secure.com

**Page 3: Campaign Metrics and Evaluation**

**Campaign Duration**: 4 Weeks

**Key Metrics to Measure Success**:

1. **Phishing Simulation Click Rate**
   * **Goal**: Reduce click-through rates on mock phishing emails from 20% baseline to below 5%.
   * **Method**: Send bi-weekly mock phishing emails to employees and track click-through.
2. **Reporting Rate**
   * **Goal**: Increase the percentage of employees who report suspicious emails to IT from 10% to 30%.
   * **Method**: Measure reports received after simulations.
3. **Training Completion Rate**
   * **Goal**: Achieve 100% completion of mandatory security training module.
   * **Method**: Track completion via LMS (Learning Management System).
4. **Pre/Post-Campaign Knowledge Assessment**
   * **Goal**: Improve average score from 60% to 85%.
   * **Method**: Administer quizzes before and after the campaign.