Social Engineering and Vishing Prevention Checklist

Use this checklist as part of your help desk security review to evaluate whether appropriate safeguards exist against impersonation-based attacks.

☐ Agents verify user identity before performing password resets, MFA resets, account unlocks, or other account recovery actions.

☐ Identity verification requirements are documented, standardized, and consistently applied across phone, email, chat, and other support channels.

☐ Callback verification is required for high-risk requests by contacting users through a trusted phone number already associated with the account.

☐ Secondary authentication measures are used before approving sensitive account changes, such as MFA resets, credential updates, or account ownership transfers.

☐ Requests involving privileged accounts, unusual account changes, or high-value customer data require additional approval before action is taken.

☐ Clear escalation procedures exist for suspicious requests, failed verification attempts, or situations where an agent cannot confidently validate a requester's identity.

☐ Support agents are trained to recognize common social engineering and vishing tactics, including impersonation attempts and information-gathering attacks.

☐ Agents are trained to identify red flags, such as urgency, pressure to bypass procedures, requests for exceptions, inconsistent account information, or unusual account recovery requests.

☐ Suspected social engineering attempts are logged, documented, and reviewed to identify trends and strengthen internal controls.

☐ Social engineering and security awareness training is reviewed and refreshed regularly to address evolving attack techniques.

☐ The organization periodically conducts phishing, vishing, or impersonation simulations to assess agent readiness and identify process gaps.

☐ Help desk staff are prohibited from bypassing identity verification procedures, regardless of the requester's claimed position, seniority, or urgency.

☐ Verification procedures require the use of information that is not publicly available or easily obtainable through social media, data breaches, or public records.

☐ Requests to change registered phone numbers, email addresses, or authentication methods are treated as high-risk and subject to enhanced verification requirements.

☐ All account recovery, credential reset, and MFA reset activities are logged and periodically reviewed for anomalies, trends, or potential abuse.