Research Report: Social Engineering Attacks Phishing, Pretexting, and Baiting

Abstract

This report examines social engineering attacks—human-focused exploits where attackers manipulate people to disclose information or take actions that compromise security. We cover phishing, pretexting, and baiting: how they work, their impact, representative case studies, and practical mitigations across technology, processes, and people.

1. Introduction

Social engineering leverages human psychology rather than software vulnerabilities. As organizations harden technical controls, attackers increasingly rely on deception: crafting believable messages, exploiting trust, and using social context to bypass defenses. Preventing social engineering requires blending awareness, detection, verification, and resilient processes.

2. Types of Social Engineering Attacks

2.1 Phishing

Phishing uses email, SMS, or messaging to trick recipients into revealing credentials, downloading malware, or taking financial actions. Variants include spear-phishing (targeted), whaling (executive-focused), and Business Email Compromise (BEC). Phishing is one of the most common initial access vectors in breaches.

2.2 Pretexting

Pretexting involves fabricating a believable scenario to obtain information or actions from a target—for example, pretending to be IT support or a vendor to request password resets or wire transfers. The attacker builds rapport and leverages authority or urgency.

2.3 Baiting

Baiting offers something enticing—physical (USB drives) or digital (free downloads)—that, when accepted, infects endpoints or exposes data. Baiting preys on curiosity or convenience and can bypass technical controls if users connect compromised media or install malicious files.

3. Case Studies and Real-world Examples

3.1 RSA SecurID (2011) — Spear Phishing

In 2011, attackers used a spear-phishing email with a malicious Excel attachment to breach RSA, the maker of SecurID tokens. The attackers stole information used later in further intrusions affecting defense contractors. The attack demonstrated how targeted phishing can defeat even security-conscious organizations.

3.2 Target Breach (2013) — Vendor Phishing/Compromise

The 2013 Target breach began when attackers phished credentials from an HVAC vendor, then used those credentials to move into Target's network and install POS malware, leading to tens of millions of customer payment records stolen. This case shows supply-chain risk from social engineering against third parties.

3.3 Ubiquiti (2015) — CEO Fraud / BEC

Ubiquiti disclosed a costly social-engineering-based financial fraud where attackers impersonated company executives and tricked employees into transferring funds—highlighting Business Email Compromise (BEC) risks and the monetary impact of fraud.

3.4 Twitter (2020) — Employee Social Engineering

In July 2020, attackers used social engineering against Twitter employees to gain access to internal admin tools and take over high-profile accounts, which were then used to run a bitcoin scam. The incident demonstrated how targeting a small number of privileged insiders can produce outsized impact.

4. Impact on Organizations

Social engineering can cause credential theft, unauthorized access, financial loss, regulatory fines, reputational damage, and downstream attacks (ransomware, data exfiltration). It often bypasses network defenses because it exploits legitimate credentials or human trust.

5. Recommendations and Preventive Measures

People & Training

- Regular, role-based security awareness training with phishing simulations.
- Teach verification steps: out-of-band confirmation for wire transfers, verifying unexpected requests with a known contact method.
- Reduce privileges and enforce least privilege to limit damage from compromised accounts.

Process & Policy

- Strict verification processes for financial requests (dual-approval, confirmed payment procedures).

• Strict verification processes for financial requests (dual-approval, confirmed payment procedures).
• Vendor security requirements and regular third-party risk assessments.
• Incident response playbooks for suspected phishing and fraud, including immediate password resets and account forensics.

Technology & Detection

• Email authentication (SPF, DKIM, DMARC) with reject/quarantine policies and BEC detection rules.
• Multi-factor authentication (prefer phishing-resistant methods such as FIDO2), conditional access, and adaptive risk-based controls.
• Endpoint protection, EDR, and blocking of autorun from removable media; disable USB autorun where possible.
• Simulated phishing, email filtering, URL sandboxing, and robust logging/monitoring to detect suspicious behavior quickly.

6. Incident Response and Recovery

• Have playbooks for credential compromise, BEC, and insider-targeted attacks: immediate revocation, containment, and forensic analysis.
• Preserve evidence for law enforcement and regulatory reporting; notify affected stakeholders promptly.
• Post-incident: root cause analysis, process hardening, and targeted remediation (e.g., remove vendor access until validated).

7. Conclusion

Social engineering remains one of the most effective attack vectors because it targets human trust. A balanced program of user education, strong authentication, process controls, and detection reduces risk. Regular testing, supplier controls, and rapid incident response are essential.

References

1. CISA - Avoiding Social Engineering and Phishing Attacks. (cisa.gov).
2. CISA - Phishing Guidance: Stopping the Attack Cycle at Phase One (2023).
3. IBM - What Is Pretexting?
4. Keepnet Labs / EasyDMARC - Baiting explanations and examples.
5. Wired - RSA SecurID breach analysis.
6. Columbia Case Study - Target 2013 breach.
7. Krebs on Security - Ubiquiti social engineering theft.
8. Twitter Investigation / NY DFS report - July 2020 compromise.
9. Verizon DBIR - Social Engineering trends and stats.