# Report On Social Engineering Attacks

### **1. Defining Social Engineering: The Art of Human Hacking**

In the context of information security, social engineering is the use of psychological influence to manipulate individuals into performing actions or divulging confidential information. It is a deceptive tactic that exploits human behavior, trust, and emotion rather than technical flaws. Attackers employ a range of communication channels, including the telephone, internet, and even in-person interactions, to coerce a victim into acting against their best interests or the best interests of their organization. The primary goal is to trick a user into disclosing sensitive data, such as account passwords, financial details, or system access credentials, which the attacker can then leverage for unauthorized access or financial fraud.This method is uniquely effective because it circumvents firewalls, anti-virus software, and other technological barriers by making a trusted user the point of compromise.

#### **1.2. The Psychological Framework: Principles of Influence**

Social engineering's effectiveness is rooted in its ability to exploit fundamental human psychological principles. Behavioral psychologist Robert Cialdini's six Principles of Influence provide a robust framework for understanding these manipulative tactics. A common thread in most social engineering schemes is the creation of a sense of

**urgency or scarcity**. The attacker pressures the target to act quickly and without careful thought, making it difficult to verify the legitimacy of the request. Attackers also frequently leverage

**authority** by impersonating trusted figures, such as senior executives, government officials, or bank representatives, to instill a sense of trust and compliance.

Other principles, such as **liking and social proof**, are used to build rapport. An attacker might impersonate a friend or colleague to gain a target's trust or reference a trusted group or trending topic to make their approach seem more authentic. Lastly, the principle of

**reciprocity** is exploited in "quid pro quo" and "baiting" attacks, which promise a service or reward in exchange for a compromising action, appealing to the human desire to return a favor or capitalize on a perceived opportunity.

#### **1.3. The Anatomy of a Social Engineering Attack**

The execution of a social engineering attack is typically a phased process that begins long before the initial contact with a target. This structured approach makes modern attacks far more sophisticated than simple, generic scams. The initial phase is **reconnaissance**, which involves extensive research on the target organization and its employees. Threat actors scour publicly available information from social media platforms like LinkedIn, Facebook, and Instagram to craft a believable backstory.This preparatory stage is crucial, as the more personal and specific the information gathered, the more convincing the subsequent deception will be. The quality of this initial information gathering directly determines the success of the entire campaign.

### **2. A Taxonomy of Social Engineering Attack Vectors**

Social engineering is not a single attack type but a broad category of deceptive practices. While each method has unique characteristics, they often overlap and can be combined to create a more potent and convincing attack.

#### **2.1. Phishing: The Digital Lure**

Phishing is a highly prevalent social engineering method that uses fraudulent electronic messages to deceive victims into revealing sensitive information.The most common form,**email phishing**, involves attackers creating fake domains that mimic legitimate organizations.These fraudulent emails often contain a sense of urgency, pressuring recipients to update account information or click on a malicious link to resolve an issue.

More targeted variants of this attack have emerged to increase success rates. **Spear phishing** targets a specific individual or group within an organization using personalized information about the victim, such as their name, job title, and employer.

**Whaling** is an even more specialized form of spear phishing that targets high-level executives, such as a CEO or CFO.The attacks are often subtler, exploiting the victim's authority and trust to get them to comply with a fraudulent request, such as a wire transfer, without questioning it.

**Smishing** involves phishing via SMS text messages, often using shortened URLs to entice victims to click.The use of smishing has increased significantly, with attackers leveraging the rise of digital services and delivery notifications to create convincing lures. Similarly,**vishing**, or "voice phishing," uses phone calls to impersonate a organization and trick individuals into providing personal information. The growing number of social media users has also given rise to **angler phishing**, where attackers hijack customer complaints on platforms like Twitter and Instagram to ask for personal details via direct message under the guise of customer support.

#### **2.2. Pretexting: The Art of the Deceptive Narrative**

Pretexting is a highly sophisticated form of social engineering where an attacker creates a plausible, fabricated scenario to manipulate a victim into divulging sensitive information. This method differs from traditional phishing in its deep reliance on a convincing narrative and the establishment of trust. The attacker's success hinges on their ability to create a believable backstory and build rapport with the victim over a period of time.

#### **2.3. Baiting: Exploiting Curiosity and Greed**

Baiting attacks lure a target into a trap by promising something appealing, such as a prize, a free download, or a reward, in exchange for a compromising action. This tactic preys on human curiosity and the temptation of something for nothing.

**Digital baiting** is the most common form, often delivered through fake advertisements, pop-up notifications, or fake online contests that trick users into downloading malware or entering credentials.

A classic and still effective method is **physical baiting**, where an attacker leaves an infected physical object, such as a USB drive or a package with a malicious QR code, in a public area hoping a curious victim will find it and plug it into their machine.This simple method can silently install malware, giving the attacker access to sensitive systems.The Stuxnet incident, where infected USB drives were used to infiltrate Iranian nuclear facilities, remains one of the most famous examples of physical baiting.

The following table provides a comparative taxonomy of the attacks discussed:

**Table 1: A Comparative Taxonomy of Social Engineering Attacks**

| Attack Type | Primary Delivery Method | Target Profile | Psychological Leveraged |
| --- | --- | --- | --- |
| Phishing | Email | Mass Audience | Urgency, Fear, Curiosity |
| Spear Phishing | Email, Phone Call | Specific Individual/Group | Authority, Trust, Urgency |
| Whaling | Email, Phone Call | Senior Executive | Authority, Fear |
| Smishing | SMS/Text Message | Mass Audience | Urgency, Trust |
| Vishing | Phone Call (VoIP) | Mass Audience/Individual | Authority, Fear, Trust |
| Pretexting | In-person, Phone Call, Email | Specific Individual | Trust, Authority, Rapport |
| Baiting | Digital (links, ads), Physical (USB) | Mass Audience | Curiosity, Greed, Urgency |

### **3. Case Studies: The Real-World Impact on Organizations**

The success of social engineering attacks is best understood by examining real-world incidents. These case studies reveal that the financial and reputational damage can be immense, often disproportionate to the technical complexity of the attack itself.

#### **3.1. Financial Deception & Business Email Compromise (BEC)**

The **2017 Google and Facebook BEC scam** is a stark example of a social engineering attack's financial impact. An attacker, Evaldas Rimasauskas, impersonated a trusted hardware vendor, Quanta Computer, and sent fraudulent invoices to employees at both companies who managed large transactions. By leveraging detailed knowledge of corporate invoicing systems and forging executive signatures and corporate seals, he deceived employees into wiring over $100 million into his fraudulent bank accounts. This incident highlights that detailed reconnaissance and a convincing pretext can easily bypass due diligence and standard financial controls.

#### **3.2. Credential Theft and System Access**

In 2014, a spear-phishing campaign against **Sony Pictures Entertainment** tricked employees into disclosing their login credentials, leading to a massive data breach and the leak of unreleased films. A single successful manipulation provided the initial access needed to cause immense financial damage and public embarrassment. Similarly, the **2020 Twitter account takeover** used a combination of phone spear phishing and pretexting to deceive Twitter employees into providing credentials that gave the attackers access to critical internal systems.This attack resulted in the compromise of over 100 high-profile accounts, including those of Barack Obama and Bill Gates, for a Bitcoin scam. Both of these incidents demonstrate that the true point of failure was not a technical vulnerability but the human element, which allowed attackers to circumvent sophisticated digital defenses.

#### **3.3. The Rise of Supply Chain and Third-Party Attacks**

Attackers are increasingly targeting third-party vendors as a way to access a larger organization. In the **2013 Target data breach**, the initial point of entry for the attackers was a third-party refrigeration contractor.By compromising this vendor, the attackers were able to infiltrate Target's network and steal credit card information from millions of customers.

This trend has continued to evolve. The **2025 ShinyHunters campaign** used social engineering to exploit weaknesses in third-party cloud platforms, specifically Salesforce.The hacking group impersonated IT support staff and tricked employees at companies like Google, TransUnion, and Air France/KLM into approving a malicious application linked to the platform.This led to the exposure of sensitive customer data at each company, including the Social Security numbers of over 4.4 million U.S. individuals from TransUnion alone. These case studies highlight a significant vulnerability: an organization's security posture is only as strong as its weakest link, which is often a third-party partner or vendor.

**Table 2: Key Social Engineering Case Studies and Their Impact**

| Attack Name/Year | Targeted Organization(s) | Method Used | Quantified Impact |
| --- | --- | --- | --- |
| Google/Facebook BEC (2017) | Google, Facebook | Business Email Compromise (BEC) | Over $100 million in financial loss |
| Sony Pictures Hack (2014) | Sony Pictures Entertainment | Spear Phishing | Theft and leak of unreleased films |
| Twitter Account Takeover (2020) | Twitter | Phone Spear Phishing, Pretexting | Compromise of over 100 high-profile accounts, including a Bitcoin scam |
| FACC AG BEC (2016) | FACC AG | BEC, CEO Impersonation | Financial loss of approximately $54 million |
| UK Energy Firm Deepfake (2019) | UK Energy Firm | AI Voice Impersonation (Vishing) | Financial loss of €220,000 |
| ShinyHunters Campaign (2025) | Google, TransUnion, Air France/KLM | Third-Party Impersonation, Pretexting | Exposure of sensitive data from millions of customers |

### **4. Recommendations: Fortifying Defenses Against Human Hacking**

A robust defense against social engineering requires a holistic strategy that integrates technical and procedural safeguards with a strong, human-centric security culture.

#### **4.1. The Critical Role of Human-Centric Controls**

The evidence suggests that 70% to 90% of all malicious data breaches involve social engineering or phishing. Therefore, focusing on the human element is paramount.

**Security awareness training (SAT)** is one of the most powerful and cost-effective defenses available.Training should be continuous, engaging, and interactive, using videos and real-life scenarios to prepare employees for the tactics they may encounter.This education should be reinforced with regular

**phishing and social engineering simulations** to test employee readiness and provide crucial metrics on human risk.

One of the most vital components of this approach is fostering a **positive security culture**. It is imperative that organizations avoid shaming employees who fall for an attack. When employees fear punishment or embarrassment, they are more likely to hide a mistake, which can prevent an organization from detecting and mitigating a breach in its early stages. By creating an environment where employees feel empowered and safe to report suspicious activity or an error, an organization turns its human workforce into a proactive layer of defense. This cultural shift is not merely a soft human resources initiative; it is a fundamental security control that strengthens the entire defense posture.

#### **4.2. Technical and Procedural Safeguards**

While human controls are critical, they must be supported by a strong technical infrastructure. The first line of defense is **advanced email filtering**, which uses artificial intelligence, machine learning, and natural language processing to detect and block sophisticated, multi-part phishing attempts before they reach an employee's inbox.

**Multi-factor authentication (MFA)** is another essential safeguard that provides an additional layer of security by requiring a second form of verification beyond a username and password.

**Conclusion: A Path to Proactive Security**

Social engineering represents the most significant threat to enterprise security because it targets the one vulnerability that cannot be patched with software: the human element. The analysis of sophisticated attacks like the 2025 ShinyHunters campaign and the Google/Facebook BEC scam reveals that the most catastrophic breaches often begin with a simple act of deception. The attacks will continue to evolve, leveraging new technologies like AI to become more convincing and harder to detect.

A resilient defense against this persistent threat requires a multifaceted approach. Organizations must move beyond a purely technical security strategy and invest in their most valuable and vulnerable asset: their people. By implementing a layered strategy of robust technical controls, continuous security education, and a positive, non-punitive culture that empowers employees to question and report suspicious activity without fear, organizations can transform their human risk from a point of failure into a powerful line of defense.

#### Works cited

1. en.wikipedia.org, accessed September 13, 2025, <https://en.wikipedia.org/wiki/Social_engineering_(security)>
2. Social engineering – ITSAP.00.166 - Canadian Centre for Cyber Security, accessed September 13, 2025, <https://www.cyber.gc.ca/en/guidance/social-engineering-itsap00166>
3. What Is Pretexting? Definition, Examples and Attacks - Fortinet, accessed September 13, 2025, <https://www.fortinet.com/resources/cyberglossary/pretexting>
4. Social Engineering Education | CDE - Colorado Department of Education, accessed September 13, 2025, <https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation>
5. www.cde.state.co.us, accessed September 13, 2025, [https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation#:~:text=Social%20Engineering%20relies%20heavily%20on,Authority%2C%20Likin](https://www.cde.state.co.us/dataprivacyandsecurity/socialengineeringeducation#:~:text=Social%20Engineering%20relies%20heavily%20on,Authority%2C%20Liking%2C%20and%20Scarcity.)