# 15 Types of Social Engineering Attacks

By SentinelOne

Published: 2024-10-18 · Archived: 2026-04-29 02:07:59 UTC

Social engineering attacks are perhaps one of the largest threats that people and companies have to face in this fast-developing digital environment. While typical cyberattacks revolve around conquering software or network vulnerabilities, key types of social engineering attacks exploit the most fragile link of all: the human. The attackers exploit natural tendencies like trust, curiosity, fear, or pressure among human beings to make them compromise and provide sensitive information or take actions that would compromise not only their security but also the security of the organization at large. In fact, 98% of cyberattacks rely on social engineering tactics and demonstrate just how much on manipulating human behavior attackers depend to achieve their goals.

A broad category of malicious attacks is based on deception and human interaction, where attackers portray themselves as trusted entities so that victims are convinced to reveal confidential information or bypass their security checks. These forms include but are not limited to, phishing emails, fraudulent phone calls, and in-person impersonations thriving in any environment lacking security awareness. With advancing technology also comes advanced social engineering tactics, which makes detection and defense increasingly difficult. It is exactly these methods that people and businesses must understand to further secure their data and systems in an inherently connected world.

In this article, we discuss what social engineering attacks are and take a deeper dive into the details of various forms of social engineering attacks.

Social engineering attacks exploit human psychology to allow confidential information or to influence the behavior of individuals compromising their security. Social engineering is entirely different from traditional hacking, as it depends more on deception or persuasion using multiple means. Just as technology changes, so do cyber criminals' tactics. Thus, the most important tool for protection is awareness and education. The most common types of social engineering attacks are listed below, each with unique methods and objectives:

1. **Phishing**: Phishing is one of the most common forms of social engineering attacks. This attack involves malicious emails, messages, or websites designed to unleash sensitive information from victims. Most often, the scams portray themselves under the identity of a legitimate source such as a bank account or an honest company, thereby deceiving people to click on malicious links or even provide their personal credentials. The resultant output can cause identity theft, financial loss, or unauthorized access to sensitive data. Mass-phishing attacks are sent out to millions of recipients for the cause of higher probability. The victims caught through phishing attacks could get their sensitive information stolen by thieves which will lead to identity theft, unauthorized access, or financial fraud.
2. **Spear Phishing**: Spear phishing is a more targeted form of phishing. Here, cyber attackers have conducted deeper research on individuals or organizations to come up with messages that are highly personalized in a way that would raise their chances of success. General phishing attacks, which are usually dispatched en bloc, tend to focus on high-value targets such as executives or key employees. Such attacks can be very

devastating as they would form the basis of corporate espionage or stealing critical data. The problem is that spear phishing can be so customized that even cautious people may become victims of phishing attacks and divulge confidential information. Most spear phishing attacks are converted into successful corporate espionage or business-sensitive data thefts if they breach internal systems. Compromising a whole organization's security often happens after breaking into the internal systems.

3. **Vishing (Voice Phishing):** Vishing is a type of phishing that uses voice communication, usually via telephone, to extract sensitive data from a victim. The cyber attackers will pretend to be authoritative figures or people that the victim entrusts, such as bank representatives or government officers, to convince the victims to hand over their personal data. Since the process uses voice interaction, which can come across as more personal and authentic than computer-based phishing attacks, it may tend to be particularly effective in cases of vishing, especially when the caller ID of the attackers is spoofed. Since vishing also relies considerably on human interaction, at times the attack can appear more legitimate or true than cyber phishing. The spoofed caller IDs are also a part of deception in this type of attack. Calls are viewed to be coming from legitimate sources based on the displayed information for call ID.
4. **Smishing (SMS Phishing):** This is yet another method of phishing. It is a technique targeted by cyber hackers wherein he or she forward short text messages, commonly referred to as SMS, that are in the name of some trusted source or may be claiming to contain a link for opening the website. The SMS directly asks users to enter personal information or download malware installed on the system. The mobile device is handy for smishing because people respond to texts very quickly as they do not respond similarly to emails. Smishing is far more accessible for attackers to exploit mobile phones because people respond instantly to text messages instead of email. The immediacy of an SMS makes users react without thinking. Meanwhile, smishing links can lead them to websites pretending to be from genuine organizations and trick victims into handing over their personal information.
5. **Pretexting**: Pretexting is when the attacker creates a scenario or pretext to get the victim to give him access or information. For instance, he might claim to be a colleague, IT support, or even law inquiring about sensitive information since it forms part of legitimate business activities. The success of pretexting depends on how well the attacker establishes trust and credibility within the victim. The success of pretexting depends on the attackers' ability to establish trust and credibility with their victims. Using their exploitation of the desire to help or to comply with the practice of authority, attackers may extract valuable data such as login credentials or personal identification. Pretexting, therefore, is a way in which there are serious breaches of data, especially in corporate environments in which unwitting employees unknowingly grant unauthorized access.
6. **Baiting**: Baiting lures victims in by making promises of something they desire, such as free software, free music, music or even money. Attackers may use physical bait, such as leaving a USB drive in a public place. When unsuspecting people insert the drive into their computers, it installs malware which lets attackers gain access to the system. Free or desirable items may allure victims into making risky decisions. Baiting actually makes use of human curiosity or greed to lure the victims to dangerous decisions. After malware is installed through such a bait, it will be possible to breach the security of whole networks. Due to this, it may eventually breach many forms of security associated with the computer. Baiting attacks may also be found in cyberspace, where users are tricked into downloading files that appear to be perfectly legitimate but contain hidden malware.

7. **Quid Pro Quo:** In quid pro quo attacks, an attacker will provide a service or benefit in exchange for information. A classic example of this is when a cybercriminal appears to be IT support, claiming that he will fix some problem with the system but insists on having the credentials of the victim's account beforehand. This technique works based on the victims' desire to be assisted or supported in order to make it easier for attackers to get their sensitive information. Quid pro quo attacks exploit the fact that a victim needs some type of assistance or aid, which makes the victim more likely to provide confidential data. Once the attackers obtain these credentials, they can access systems, extract information, or install malicious code on computers. This is extremely dangerous in any corporate environment where the employees are eager to have technical issues resolved as fast as possible.
8. **Tailgating (Piggybacking):** Tailgating is a physical social engineering attack in which an unauthorized person follows an authorized user into a restricted area. For instance, it might be that a person accompanies an employee through a door after he professes to have forgotten his access card. Thus, attackers can gain entry into areas from where they are not supposed to gain entry and may even commit data breaches or theft. Once inside, the hacker can go to areas to which they are not allowed, risking theft of sensitive information, breach of data, and even sabotage. Tailgating exploits the victim's niceness or willingness to help, making it a rather simple yet effective way to overcome physical security controls. This kind of attack shows that access control must be strictly enforced in secure environments.
9. **Dumpster Diving**: Dumpster diving is a hack where attackers dig into the dumpster for account numbers, password numbers, or other sensitive information. It is usually used to gain insights that can be applied in a second attack, often in phishing or pretexting. Organizations must ensure proper disposal and must prevent the chance of attacking through this method. Dumpster diving can at times go unnoticed, but it certainly contains a lot of information that could be revealed to attackers. A paper used within any organization should therefore be disposed of properly, such as shredding and secure deletion of sensitive data, in order not to fall under this kind of attack. Even the smallest, seemingly irrelevant details can assist an attacker in engineering more complex social engineering attacks.
10. **Watering Hole Attack**: In a watering hole attack, cybercrime attackers hack into those websites that are mainly visited by a specific group or organization. The malware-infected website injects malware into the laptops of its visitors who download it blindly into their systems. The attack is targeted at a group of users and is particularly dangerous for organizations whose users have a shared digital environment. Watering hole attacks are highly targeted and appear especially dangerous to an organization for shared common digital platforms. The malware goes undetected to steal massive amounts of data or compromise a system completely. These attacks leverage the trust associated with familiar websites, requiring highly advanced cybersecurity measures to identify.
11. **Business Email Compromise (BEC):** Business Email Compromise is a targeted attack whereby cyber scammers compromise legitimate business email accounts so that employees are tricked into transferring money or sensitive information. Many times, it is presented as high-level executives and creates an urgency to compel acceptance. BEC attacks are destructive, which not only cause loss of money but also theft of information. Therefore, it is especially convincing to use legitimate email addresses used by attackers. Businesses should instill strict rules for email security, such as multi-factor authentication, to ward off such BEC attacks.
12. **Honey Trap**: Attackers engage victims in an emotional chat over the internet, which is also referred to as a honey trap. Once contact is initiated, victims fall into the attacker's trap by sharing passwords, corporate

secrets, or even money. Honey trap exploit victims' emotions, making them more susceptible to manipulation. It becomes very personalized since an attacker takes weeks or months to win trust and then attacks. These attacks can lead to wide-scale personal and financial losses if the victim is employed in a sensitive role within an organization.

13. **Rogue Security Software:** Cyber attackers take spurious security software that looks like authentic ones and reports fake malware infections in users' computers. Once downloaded, the software installs the very malware, and it ends up stealing data or demanding money for ransom. Fear is their only reliance since they use popups that never stop and security warnings forcing someone to act really fast. Thereby, sensitive information leaks out or payments are made to a cybercrime situation that does not exist at all. This attack can leave the real antivirus programs irrelevant, and thus, make the system vulnerable. The victim may receive identity theft or data breaches; data thefts relating to financial information, for instance.
14. **Social Media Exploitation**: This highly connected world makes social networking sites essential media for information, communication, and relationships. On the other hand, they leave fertile ground for nefarious or malicious persons who take advantage of or use users for their agendas. Cybercriminals are known to gather information and intelligence on their targets through social networking sites, manipulating or deceiving people in a lot of different tactics to reveal sensitive data to themselves. One of the most common deceptions is the use of phantom profiles or presenting oneself as known people-friends, relatives, colleagues, and even institutional or authoritative organizations.
15. **Impersonation**: Impersonation attacks occur when attackers pretend to be a known or trusted person, such as an IT staff member or manager, for the purpose of accessing systems or data. They exploit the perceived trust that exists between the victims and the perceived authority figures. Attackers often use actual names, insider information, or corporate jargon to masquerade as authentic, making it challenging to detect the forgery. Once one gets access to trusted areas, they may acquire sensitive systems or data and even serious security breaches or theft of confidential information. Impersonation in most cases results in serious consequences if the attacker reaches the restricted areas or sensitive accounts.

Prevention of social engineering attacks requires education, technology, and defined processes in a proactive manner. Cybercriminals operate based on the manipulation of human psychology; hence, security awareness becomes very important within an organization. Here are some effective strategies to mitigate the risk of social engineering attacks:

- **Employee Training:** Educating the employees regarding the tactics in social engineering attacks helps build a security-conscious culture. Even regular training sessions might enable the persons to identify suspicious behavior, understand all the different forms of social engineering, and avoid falling into common scams. Interactive learning methods, such as simulated phishing exercises, help to reinforce learning and prepare employees to respond effectively when they encounter potential threats. Ongoing education will keep employees updated with the latest tactics cybercriminals use.

- **Use Multi-Factor Authentication (MFA):** This makes it much more difficult for an attacker to gain access when using Multi-Factor Authentication. In the case of a stolen login credential, MFA will require another method of verification—such as a one-time code sent to a mobile device or biometric recognition—to complete the login process. Using MFA reduces an organization's overall risk of unauthorized access to systems and data.

- **Verify Requests for Sensitive Information:** All requests for sensitive information must be verified. This especially comes in when the source or channel is unknown. In this case, employees should be specially alerted with respect to the approaches taken toward receiving such requests via emails, phone calls, or even text messages. They must be cautious and properly verify it before releasing the sensitive information through direct contacting of the requester via a known number or else contacting a supervisor contact.
- **Implement Email Filtering Solutions:** Apply advanced email filtering techniques that can detect phishing emails and other suspicious messages before they actually land in the employee's inbox. Email filters, based on pre-defined factors, could pick up on potential malicious content, including phishing links or attachments, and flag it for further investigation. Regular updates and fine-tuning of filters ensure sophisticated filtering that avoids successful phishing attempts and rectifies the threat.
- **Limit Access to Sensitive Information:** The principle of least privilege should be implemented throughout the organization, with access to sensitive data and systems granted to only those who have genuine reasons to access them. This mitigates the impact if an attacker succeeds in unauthorized access. Regular reviews and updates of access permissions based on role and responsibilities ensure the abrupt removal of outdated access rights.
- **Monitor for Unusual Activity:** Keep a sharp eye on network activity and user behavior, especially looking for malicious activity such as unauthorized login, unusual data access patterns, or suspicious file transfers. SIEM tools can support real-time anomaly detection by organizations. Alerts based on suspicious behavior also allow organizations to quickly respond to the threat before it becomes more severe.

For more detail, read: How to Prevent Social Engineering Attacks

### Enhance Your Threat Intelligence

See how the SentinelOne threat-hunting service WatchTower can surface greater insights and help you outpace attacks.

Learn More

## Conclusion

With social engineering attacks growing and becoming increasingly persistent in the modern cybersecurity environment, it is imperative that more depth be given to today's threats. Social engineering attacks are one of those attacks, from the most straightforward forms, such as phishing and pretexting, to advanced attacks like spear phishing and watering hole attacks, which exploit human psychology and social interactions to gain unauthorized access to sensitive information or systems.

Again, prevention begins with awareness and training of employees. These risks will be significantly minimized if there is a security-conscious culture in combination with sound security measures such as multi-factor authentication, email filtering, and network monitoring.

---

Source: https://www.sentinelone.com/cybersecurity-101/threat-intelligence/types-of-social-engineering-attacks/