What is Social Engineering?

Social Engineering Definition

Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions.

Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information.

Generally, social engineering attackers have one of two goals:

1. Sabotage: Disrupting or corrupting data to cause harm or inconvenience.
2. Theft: Obtaining valuables like information, access, or money.

This social engineering definition can be further expanded by knowing exactly how it works.

How Does Social Engineering Work?

Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.

The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows:

1. **Prepare** by gathering background information on you or a larger group you are a part of.
2. **Infiltrate** by establishing a relationship or initiating an interaction, started by building trust.
3. **Exploit the victim** once trust and a weakness are established to advance the attack.
4. **Disengage** once the user has taken the desired action.

This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.

It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts.

By masquerading as legitimate users to IT support personnel, they grab your private details — like name, date of birth or address. From there, it's a simple matter to reset passwords and gain almost unlimited access. They can steal money, disperse social engineering malware, and more.

Traits of Social Engineering Attacks

Social engineering attacks center around the attacker's use of persuasion and confidence. When exposed to these tactics, you are more likely to take actions you otherwise wouldn't.

Among most attacks, you'll find yourself being misled into the following behaviors:

Heightened emotions: Emotional manipulation gives attackers the upper hand in an any interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state. The following emotions are all used in equal measure to convince you.

- Fear
- Excitement
- Curiosity
- Anger
- Guilt
- Sadness

Urgency: Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly. Either approach overrides your critical thinking ability.

Trust: Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately lying to you, confidence plays an important role here. They've done enough research on you to craft a narrative that's easy to believe and unlikely to rouse suspicion.

There are some exceptions to these traits. In some cases, attackers use more simplistic methods of social engineering to gain network or computer access. For example, a

hacker might frequent the public food court of a large office building and "shoulder surf" users working on their tablets or laptops. Doing so can result in a large number of passwords and usernames, all without sending an email or writing a line of virus code.

Now that you understand the underlying concept, you're probably wondering "what is social engineering attack and how can I spot it?"

Types of Social Engineering Attacks

Almost every type of cybersecurity attack contains some kind of social engineering. For example, the classic email and virus scams are laden with social overtones.

Social engineering can impact you digitally through mobile attacks in addition to desktop devices. However, you can just as easily be faced with a threat in-person. These attacks can overlap and layer onto each other to create a scam.

Here are some common methods used by social engineering attackers:

Phishing Attacks

Phishing attackers pretend to be a trusted institution or individual in an attempt to persuade you to expose personal data and other valuables.

Attacks using phishing are targeted in one of two ways:

1. **Spam phishing,** or mass phishing, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person.

2. **Spear phishing** and by extension, **whaling** , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.

Whether it's a direct communication or via a fake website form, anything you share goes directly into a scammer's pocket. You may even be fooled into a malware download containing the next stage of the phishing attack. Methods used in phishing each have unique modes of delivery, including but not limited to:

Voice phishing (vishing) phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you to increase trust and urgency.

SMS phishing (smishing) texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number.

Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

Angler phishing takes place on social media, where an attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack.

Search engine phishing attempt to place links to fake websites at the top of search results. These may be paid ads or use legitimate optimization methods to manipulate search rankings.

URL phishing links tempt you to travel to phishing websites. These links are commonly delivered in emails, texts, social media messages, and online ads. Attacks hide links in hyperlinked text or buttons, using link-shortening tools, or deceptively spelled URLs.

In-session phishing appears as an interruption to your normal web browsing. For example, you may see such as fake login pop-ups for pages you're currently visiting.

Baiting Attacks

Baiting abuses your natural curiosity to coax you into exposing yourself to an attacker. Typically, potential for something free or exclusive is the manipulation used to exploit you. The attack usually involves infecting you with malware.

Popular methods of baiting can include:

- USB drives left in public spaces, like libraries and parking lots.
- Email attachments including details on a free offer, or fraudulent free software.

Physical Breach Attacks

Physical breaches involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information.

Attacks of this nature are most common in enterprise environments, such as governments, businesses, or other organizations. Attackers may pretend to be a representative of a known, trusted vendor for the company. Some attackers may even be recently fired employees with a vendetta against their former employer.

They make their identity obscure but believable enough to avoid questions. This requires a bit of research on the attacker's part and involves high-risk. So, if someone is attempting this method, they've identified clear potential for a highly valuable reward if successful.

Pretexting Attacks

Pretexting uses a deceptive identity as the "pretext" for establishing trust, such as directly impersonating a vendor or a facility employee. This approach requires the attacker to interact with you more proactively. The exploit follows once they've convinced you they are legitimate.

Access Tailgating Attacks

Tailgating , or piggybacking, is the act of trailing an authorized staff member into a restricted-access area. Attackers may play on social courtesy to get you to hold the door for them or convince you that they are also authorized to be in the area. Pretexting can play a role here too.

Quid Pro Quo Attacks

Quid pro quo is a term roughly meaning "a favor for a favor," which in the context of phishing means an exchange of your personal info for some reward or other compensation. Giveaways or offers to take part in research studies might expose you to this type of attack.

The exploit comes from getting you excited for something valuable that comes with a low investment on your end. However, the attacker simply takes your data with no reward for you.

DNS Spoofing and Cache Poisoning Attacks

DNS spoofing manipulates your browser and web servers to travel to malicious websites when you enter a legitimate URL. Once infected with this exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.

DNS cache poisoning attacks specifically infect your device with routing instructions for the legitimate URL or multiple URLs to connect to fraudulent websites.

Scareware Attacks

Scareware is a form of malware used to frighten you into taking an action. This deceptive malware uses alarming warnings that report fake malware infections or claim one of your accounts has been compromised.

As a result, scareware pushes you to buy fraudulent cybersecurity software, or divulge private details like your account credentials.

Watering Hole Attacks

Watering hole attacks infect popular webpages with malware to impact many users at a time. It requires careful planning on the attacker's part to find weaknesses in specific sites. They look for existing vulnerabilities that are not known and patched — such weaknesses are deemed **zero-day exploits** .

Other times, they may find that a site has not updated their infrastructure to patch out known issues. Website owners may choose delay software updates to keep software versions they know are stable. They'll switch once the newer version has a proven track record of system stability. Hackers abuse this behavior to target recently patched vulnerabilities.

Unusual Social Engineering Methods

In some cases, cybercriminals have used complex methods to complete their cyberattacks, including:

- **Fax-based phishing:** When one bank's customers received a fake email that claimed to be from the bank — asking the customer to confirm their access codes – the method of confirmation was not via the usual email / Internet routes. Instead, the customer was asked to print out the form in the email, then fill in their details and fax the form to the cybercriminal's telephone number.
- **Traditional mail malware distribution:** In Japan, cybercriminals used a home-delivery service to distribute CDs that were infected with Trojan spyware. The disks were delivered to the clients of a Japanese bank. The clients' addresses had previously been stolen from the bank's database.

Examples of Social Engineering Attacks

Malware attacks deserve a special focus, as they are common and have prolonged effects.

When malware creators use social engineering techniques, they can lure an unwary user into launching an infected file or opening a link to an infected website. Many email worms and other types of malware use these methods. Without a comprehensive security software suite for your mobile and desktop devices, you're likely exposing yourself to an infection.

Worm Attacks

The cybercriminal will aim to attract the user's attention to the link or infected file – and then get the user to click on it.

Examples of this type of attack include:

- **The LoveLetter worm** that overloaded many companies' email servers in 2000. Victims received an email that invited them to open the attached love letter. When they opened the attached file, the worm copied itself to all of the contacts in the victim's address book. This worm is still regarded as one of the most devastating, in terms of the financial damage that it inflicted.
- **The Mydoom email worm** — which appeared on the Internet in January 2004 — used texts that imitated technical messages issued by the mail server.
- **The Swen worm** passed itself off as a message that had been sent from Microsoft.

It claimed that the attachment was a patch that would remove Windows vulnerabilities. It's hardly surprising that many people took the claim seriously and tried to install the bogus security patch — even though it was really a worm.

Malware Link Delivery Channels

Links to infected sites can be sent via email, ICQ and other IM systems — or even via IRC Internet chat rooms. Mobile viruses are often delivered by SMS message.

Whichever delivery method is used, the message will usually contain eye-catching or intriguing words that encourage the unsuspecting user to click on the link. This method of penetrating a system can allow the malware to bypass the mail server's antivirus filters.

Peer-to-Peer (P2P) Network Attacks

P2P networks are also used to distribute malware. A worm or a Trojan virus will appear on the P2P network but will be named in a way that's likely to attract attention and get users to download and launch the file. For example:

- AIM & AOL Password Hacker.exe
- Microsoft CD Key Generator.exe
- PornStar3D.exe
- Play Station emulator crack.exe

Shaming Infected Users out of Reporting an Attack

In some cases, the malware creators and distributors take steps that reduce the likelihood of victims reporting an infection:

Victims may respond to a fake offer of a free utility or a guide that promises illegal benefits like:

- Free Internet or mobile communications access.
- The chance to download a credit card number generator.
- A method to increase the victim's online account balance.

In these cases, when the download turns out to be a Trojan virus, the victim will be keen to avoid disclosing their own illegal intentions. Hence, the victim will probably not report the infection to any law enforcement agencies.

As an example of this technique, a Trojan virus was once sent to email addresses that were taken from a recruitment website. People that had registered on the site received

fake job offers, but the offers included a Trojan virus. The attack mainly targeted corporate email addresses. The cybercriminals knew that the staff that received the Trojan would not want to tell their employers that they had been infected while they were looking for alternative employment.

How to Spot Social Engineering Attacks

Defending against social engineering requires you to practice self-awareness. Always slow down and think before doing anything or responding.

Attackers expect you to take action before considering the risks, which means you should do the opposite. To help you, here are some questions to ask yourself if you suspect an attack:

- **Are my emotions heightened?** When you're especially curious, fearful, or excited, you're less likely to evaluate the consequences of your actions. In fact, you probably will not consider the legitimacy of the situation presented to you. Consider this a red flag if your emotional state is elevated.
- **Did this message come from a legitimate sender?** Inspect email addresses and social media profiles carefully when getting a suspect message. There may be characters that mimic others, such as "torn@example.com" instead of "tom@example.com." Fake social media profiles that duplicate your friend's picture and other details are also common.
- **Did my friend actually send this message to me?** It's always good to ask the sender if they were the true sender of the message in question. Whether it was a coworker or another person in your life, ask them in-person or via a phone call if possible. They may be hacked and not know, or someone may be impersonating their accounts.
- **Does the website I'm on have odd details?** Irregularities in the URL, poor image quality, old or incorrect company logos, and webpage typos can all be red flags of a fraudulent website. If you enter a spoofed website, be sure to leave immediately.
- **Does this offer sound too good to be true?** In the case of giveaways or other targeting methods, offers are a strong motivation to drive a social engineering attack forward. You should consider why someone is offering you something of value for little gain on their end. Be wary at all times because even basic data like your email address can be harvested and sold to unsavory advertisers.
- **Attachments or links suspicious?** If a link or file name appears vague or odd in a message, reconsider the authenticity of the whole communication. Also, consider if the message itself was sent in an odd context, time, or raises any other red flags.

- **Can this person prove their identity?** If you cannot get this person to verify their identity with the organization, they claim to be a part of, do not allow them the access they are asking for. This applies both in-person and online, as physical breaches require that you overlook the attacker's identity.

How to Prevent Social Engineering Attacks

Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users.

Here are some important ways to protect against all types of cyberattacks:

Safe Communication and Account Management Habits

Online communication is where you're especially vulnerable. Social media, email, text messages are common targets, but you'll also want to account for in-person interactions as well.

Never click on links in any emails or messages . You'll want to always manually type a URL into your address bar, regardless of the sender. However, take the extra step of investigating to find an official version of the URL in question. Never engage with any URL you have not verified as official or legitimate.

Use multi-factor authentication. Online accounts are much safer when using more than just a password to protect them. Multi-factor authentication adds extra layers to verify your identity upon account login. These "factors" can include biometrics like fingerprint or facial recognition, or temporary passcodes sent via text message.

Use strong passwords (and a password manager). Each of your passwords should be unique and complex. Aim to use diverse character types, including uppercase, numbers, and symbols. Also, you will probably want to opt for longer passwords when possible. To help you manage all your custom passwords, you might want to use a password manager to safely store and remember them.

Avoid sharing names of your schools, pets, place of birth, or other personal details. You could be unknowingly exposing answers to your security questions or parts of your password. If you set up your security questions to be memorable but inaccurate, you'll make it harder for a criminal to crack your account. If your first car was a "Toyota," writing a lie like "clown car" instead could completely throw off any prying hackers.

Be very cautious of building online-only friendships. While the internet can be a great way to connect with people worldwide, this is a common method for social

engineering attacks. Watch for tells and red flags that indicate manipulation or a clear abuse of trust.

Safe Network Use Habits

Compromised online networks can be another point of vulnerability exploited for background research. To avoid having your data used against you, take protective measures for any network you're connected to.

Never let strangers connect to your primary Wi-Fi network. At home or in the workplace, access to a guest Wi-Fi connection should be made available. This allows your main encrypted, password-secured connection to remain secure and interception-free. Should someone decide to "eavesdrop" for information, they won't be able to access the activity you and others would like to keep private.

Use a VPN. In case someone on your main network — wired, wireless, or even cellular — finds a way to intercept traffic, a virtual private network (VPN) can keep them out. VPNs are services that give you a private, encrypted "tunnel" on any internet connection you use. Your connection is not only guarded from unwanted eyes, but your data is anonymized so it cannot be traced back to you via cookies or other means.

Keep all network-connected devices and services secure. Many people are aware of internet security practices for mobile and traditional computer devices. However, securing your network itself, in addition to all your smart devices and cloud services is just as important. Be sure to protect commonly overlooked devices like car infotainment systems and home network routers. Data breaches on these devices could fuel personalization for a social engineering scam.

Safe Device Use Habits

Keeping your devices themselves is just as important as all your other digital behaviors. Protect your mobile phone, tablet, and other computer devices with the tips below:

Use comprehensive internet security software. In the event that social tactics are successful, malware infections are a common outcome. To combat rootkits, Trojans and other bots, it's critical to employ a high-quality internet security solution that can both eliminate infections and help track their source.

Don't ever leave your devices unsecured in public. Always lock your computer and mobile devices, especially at work. When using your devices in public spaces like airports and coffee shops, always keep them in your possession.

Keep all your software updated as soon as available. Immediate updates give your software essential security fixes. When you skip or delay updates to your operating

system or apps, you are leaving known security holes exposed for hackers to target. Since they know this is a behavior of many computer and mobile users, you become a prime target for socially engineered malware attacks.

Check for known data breaches of your online accounts. Services like Kaspersky Security Cloud actively monitor new and existing data breaches for your email addresses. If your accounts are included in compromised data, you'll receive a notification along with advice on how to take action.

Protection against social engineering starts with education. If all users are aware of the threats, our safety as a collective society will improve. Be sure to increase awareness of these risks by sharing what you've learned with your coworkers, family, and friends.

Related articles:

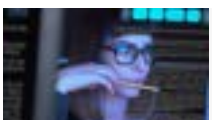
- Top 10 Most Notorious Hackers of All Time
- Mobile Malware Threats to Watch out for!
- Malware Implementation Techniques
- Malware and Exploit Detection
- Choosing an Antivirus Solution
- Malware Classifications

Featured Articles

What is extended detection and response (XDR)?

What are NFTs and how do they work?

What is hacking? And how to prevent it



How the Zero Trust concept is shaping cybersecurity at scale