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 cybersecurity, the "weakest link" is the human, and it's unsurprising 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 not further expanded by knowing exactly how it works, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can exploit and manipulate the user effectively.

In addition, hackers try to exploit a user's lack of knowledge. Thanks to the spread of technology, many consumers and employees aren't aware of certain threats like **drive-by downloads** or **malicious links**, and social engineering attacks can easily trick a unaware number. As a result, many users are unsure how to spot potential threats and their information.

Commonly, social engineering attacks 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.

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

Don't stress over passwords

Protect and remember them with a special tool included in our premium product.

Kaspersky Password Manager

Learn More

How Does Social Engineering Work?

Most social engineering attacks rely on a quick connection between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using **force tactics** to breach your data.

The attack cycle goes 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 and pick a target group you are a part of.
2. **Initiate:** 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 manipulating or exploiting 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 steal passwords, credit cards, and sensitive 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 moved into the following behaviors:

Heightened emotions: Emotional manipulation plays attackers the upper hand in 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 notable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that is time-limited if you do not act quickly. Either approach increases your risk of making a mistake.

Trust: Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately trying to pry confidential data or important crew from. They have strong enough reason to pry to craft a narrative that's easy to believe and unlikely to cause suspicion.

There are some exceptions to these traits. In some cases, attackers use more simplistic methods of social engineering to gain between or computer access. For example, a hacker might frequent the public food court of a large office building and "shoulder surf" users passwords or credit card numbers. Or they might "tailgate" or follow an authorized user into a secure area, all without sending an email or setting a line of cover story.

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

Types of Social Engineering Attacks

Across 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 your digitally through **mobile attacks** in addition to desktop devices. However, you can pick up 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 not personalized and are easier to identify and avoid.
2. **Spear phishing**: and its 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, phishing 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 such 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 site 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 sent.

Angler phishing takes place on social media, where an attacker creates a trusted company's customer service team. They intercept your communications with a brand to find out about 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 search engine optimization methods to manipulate search rankings.

URL phishing takes target you to a fake phishing website. 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 modified 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 leverages 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 trusted third party, such as a maintenance crew member, or they may trick employees with a similarly against their former employer.

The ends they transfer obtained data to attackers enough to avoid questions. This requires a lot of research on the attacker's part and involves high risk. Our if someone is attempting into, internal, physical identities pose potential for a highly valuable reward if successful.

Pretexting Attacks/Ploys

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 precisely. The exploit follows once they've convinced you they are legitimate.

Tailgating Attacks/Ploys

Tailgating, or piggybacking, is the act of making an authorized staff member into a restricted access area. Attackers may plan 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 commitment on your end. However, the attacker simply wants 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 without your knowledge. Hackers can hijack a domain name, redirect traffic to other locations, or perform the inaccurate routing data is cleared from the systems involved.

DNS cache poisoning attacks specifically affect 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. The deceptive software displays alarming and fake reports about malware infections or claim some of your accounts has been compromised.

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

Watering Hole Attacks

Watering hole attacks infect popular webpages with malware to impact many users at a time. The attacker hopes to infect the device of a particular target group they're interested in. They look for existing vulnerabilities that are not known and patched – such exploitation are deemed **zero-day exploits**.

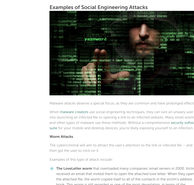
Other times, they may find that a site has not updated their infrastructure to patch out known issues. Website owners may choose delay software updates to keep software versions they know are stable. They'll switch onto the newer version has a proven track record of system stability. Hackers know this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

Unusual Social Engineering Methods

In some cases, cybercriminals have used complex methods to complete their cyberattacks. Examples include:

1. **Fax-based phishing**: When one bank's customers received a fake email that claimed to be from the bank – it directed the customers to confirm their details online. It also included a fax number to call, where the customer's internal recipient, instead, the customer was asked to print out the form or the email, then fill in their details and fax the form to the cybercriminal's telephone number.
2. **Traditional mail malware distribution**: In Japan, cybercriminals used a home delivery service to distribute CDs that were infected with Trojan spyware. The disks were addressed to the victim's home and mailed. The victim addresses had previously been scam from the bank's database.

Examples of Social Engineering Attacks



Malware attacks deserve a special focus, as they are common and have prompted others.

When **malware creators** use social engineering techniques, they can scale to unmeasured scale into launching an infected file or opening a link to an infected website. Many small actions and other types of malware attack 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 phish the victim to convince the link to be 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 with the subject line "I love you" and an attachment. 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 the victim's address book to send itself to other unsuspecting users.
- **The Sasser worm** caused hard of all 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 fell into the trap. Sasser was the fastest – 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 chat rooms. Mobile viruses are often delivered by SMS messages.

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. The method of persuading a victim 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 & ICQ, Password Hacker.exe
- Microsoft CD Key Generator.exe
- PornStarXXX.exe
- Pop Station emulator crack.exe

Diverting 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 bite offer of a free utility or a quake that promises design 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 discussing their seen illegal intentions. Hence, the victim will probably not report the attack to the authorities.

Also known as a Trojan horse, a Trojan virus was once sent to email addresses that were taken from a customer database. People that had signed up for the free Internet access 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 employments.

How to Spot Social Engineering Attacks

Defending against social engineering should not be a job for anti-sweaterness. 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 for any irregularities. Cybercriminals may use a fake email address that seems similar, such as "kondapacorp.com" instead of "kondapacorp.com." Fake social media profiles that plagiarize your friend's picture and other details are also common.
- **Did my friend actually send this message to me?** It's easy enough to ask the sender if they were the true sender of the message in question. Whether it was a coworker or family member, a quick call or text can confirm whether their account was in fact hacked and not know, or someone may be impersonating their identity online.
- **Does the website I'm on have enough data?** Investigate in the URL, page image quality, site or document company logos, and webpage copies can all be red flags of a fraudulent website. If you enter a spoofed website, be sure to leave immediately.
- **Does this offer seem too good to be true?** Free gifts, prizes, and rewards gather targeting. Ask yourself, "Did I enter any contest that would lead me to receive this prize?" If not, you should consider why someone is offering you something of value for little gain or their end. Be wary of 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 attachment or link matches what the sender would typically share with you.
- **Can this person prove their identity?** If you cannot get the 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 people and online, as physical breaches require that you continue this attacker's identity.

How to Prevent Social Engineering Attacks

Beyond spotting an attacks, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is revolving 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 also want to be careful in person or on telephone as well.

Never click on links in any emails or messages: You don't 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 vitaut spite when using more than just a password to protect them. Multi factor authentication adds some 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, complex, and difficult to guess. Avoid using personal information, common words, and patterns, since you will probably want to be "right" password. Password manager can 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 some of your passwords. If you set up your security questions to be more obscure, you can avoid this problem. Instead of using your pet's name, you could use a favorite food, hobby, or nickname. Be creative!

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. Stick to fun, bite and not too logic 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 leaving your data open and ripe for the picking, follow these measures for any network you're connected to:

Never let strangers connect to your home network: At home or in the workplace, access to a guest Wi-Fi connection should be made available. This allows your main network to remain protected and secure. Internet access and information flow through separate devices to operational. On workplace, they need to be able to access the activity and anything related to keep power.

Use a VPN: To make someone on your home network – connect remotely, or connection 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" of any internet connection you make. Your connection is not only guarded from unwanted eyes, but your data is anonymized so it cannot be traced back to you or **cookies** on other sites.

Keep all network-connected devices and services secure: Many people are aware of cybersecurity threats on their phones, laptops, and computers, but forget about securing your network itself. In addition to all your smart devices and cloud services, it is 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 frictionless is just as important as all your other digital behaviors. Protect your mobile phones, tablets, and other connected devices with the following:

Use comprehensive internet security software: In the event that social tactics are successful, malware infections are a common outcome. To combat viruses, Trojans and other bots, it's critical to employ a high-quality **internet security** solution that can both prevent infections and help recover from an attack.

Don't ever leave your devices unsecured in public: Always lock your computer and mobile devices when you're away. Be careful of "shoulder surfers" who can see your passwords and other private details.

Related Articles

What is hacking? And how to prevent it?

How the Zero Trust concept is shaping cybersecurity as we know it

What is endpoint security and how does it work?

What is a PUP?

What is zero-click malware, and how do you prevent it?

Kaspersky Premium

Premium protection for your whole digital world.

Learn More

kaspersky

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

Protecting You, Your Family & More

Get the Power to Protect. Discover how our award-winning security helps protect what matters most to you.

Get FREE Tools

There's a wide range of FREE Kaspersky tools that can help you to stay safe – on PC, Mac, iPhone, iPad & Android devices.

We're Here to Help

Helping you stay safe is what we're about – so, if you need to contact us, get answers to some FAQs or access our technical support team.

Who We Are

Find out why we're so committed to helping people stay safe... online and beyond.

Get Your Free Trial

Try Before You Buy. In just a few clicks, you can get a FREE trial of one of our products – so you can put our technologies through their paces.

Student Discount

Students save on the leading antivirus and Internet Security software with this special offer.

Stay in Touch

Home Products

Kaspersky Anti-Virus
Kaspersky Android Antivirus
Kaspersky Internet Security
Kaspersky Total Security
Kaspersky Security Cloud
Kaspersky VPN Secure Connection
Free Antivirus
All Products

Small Business Products
(1-100 EMPLOYEES)

Kaspersky Small Office Security
Kaspersky Endpoint Security Cloud
All Products

Medium Business Products
(101-999 EMPLOYEES)

Kaspersky Endpoint Security Cloud
Kaspersky Endpoint Security for Business Select
Kaspersky Endpoint Security for Business Advanced
All Products

Enterprise Solutions
(1000+ EMPLOYEES)

Cybersecurity Services
Threat Management and Defense
Endpoint Security
Hybrid Cloud Security
Cybersecurity Training
Threat Intelligence
All Solutions

© 2022 AO Kaspersky Lab. All Rights Reserved. Adaptive security technology is based on the patent US7584508 B1: 'Adaptive security for information devices'. • Privacy Policy • Online Tracking Opt-Out Guide • Anti-Corruption Policy • License Agreement B2C • License Agreement B2B

United States

Contact Us • About Us • Partners • Blog • Resource Center • Press Releases • Sitemap • Careers