Continue

Social engineering is one of the most prevalent cybercriminal tactics. According to a recent Gen Threat Report, many online attacks either begin with social engineering techniques or leverage them to spread malware. What is social engineering? Social engineering is a tactic cybercriminals use to manipulate people into divulging personal information or performing actions that compromise security. Instead of directly targeting technical systems, social engineering attacks exploit human behavior, playing on emotions like fear, trust, curiosity, or pity to steal personal and financial information. Once they obtain the information they're after, social engineers can access sensitive accounts, engage in corporate espionage, commit fraud, blackmail their victims, or sell the data on the dark web. How does social engineering work? Social engineers usually communicate directly with their victims to manipulate them into compromising their security. They may also create fake websites and pop-ups to convince large numbers of victims to hand over money or information. Social engineering typically involves the following steps: 1. Gathering background information Cybercriminals begin by gathering personal information about their victims. They may purchase data on the dark web, scour publicly available sources like social media profiles or data brokers, or exploit data breaches. They might also use phishing emails, fake surveys, or spoofed websites to trick individuals into revealing personal details to launch a more targeted social engineering attack. 2. Making contact and building trust Once the social engineer has enough information, they initiate contact via email, text, phone, or social media. They will typically pose as trustworthy figures or entities and use the information collected in step one to build credibility. 3. Exploiting the victim Next, the cybercriminal exploits the victim's emotions and manipulates them into clicking a malicious link, sending money, or revealing sensitive information. They may offer an exclusive reward, claim they need urgent help, threaten to close their victim's accounts, or warn of large charges or fees. The goal is to pressure the victim into acting quickly without fully considering the consequences. 4. Disengaging after the attack When the cybercriminal has stolen money, infected a device with malware, or obtained whatever information they were after, they disengage, often leaving the victim unaware of the breach until it's too late. Diagram showing how social engineering works. 9 types of social engineering attacks Attackers use multiple social engineering tactics to trick individuals into compromising their security. Here are examples of nine common social engineering schemes. 1. Phishing In phishing attacks, cybercriminals use fake emails, websites, calls, or messages to trick individuals into sharing sensitive information like login credentials or financial details. These scams often imitate trusted brands, like Geek Squad, creating a sense of urgency with messages like "Your account is at risk" or "Immediate action required." Numerous scams fall under the phishing category. Here are a few common types of phishing attacks. Email phishing: Scammers send fraudulent emails to trick you into revealing personal information. These emails may also include a malicious link that infects devices with malware or takes you to a dangerous website. Clone Phishing: This type of email phishing happens when a cybercriminal creates a near-exact replica of a legitimate email you've received before, modifying it to include malicious links or attachments. Spear phishing: Unlike generic phishing attacks sent out to many people at once, spear phishing targets specific individuals or organizations. This technique's personalized approach increases the message's apparent authenticity. Whaling: This form of spear phishing specifically targets high-profile individuals, such as executives or public figures. Smishing: In smishing, or SMS phishing attacks, cybercriminals try to lure people into clicking a link sent via text, a common example being fake bank texts. Vishing: Vishing is a portmanteau of voice and phishing; scammers impersonate legitimate organizations or individuals over the phone. Quishing: Quishing attacks use fake QR codes to trick victims into visiting malicious websites. Cybersecurity tip: One way to identify phishing emails or text messages is poor spelling and grammar. Legitimate organizations work with professional copywriters to ensure communication is clear and error-free. 2. Baiting Baiting is a social engineering tactic where scammers lure people into downloading malware or sharing personal information by piquing their curiosity or using tempting offers like exclusive deals or free downloads. Once downloaded, the malware can steal personal data that scammers can sell on the dark web or use to commit various types of identity theft. Criminals use multiple baiting techniques to trick individuals. Here are a few common types of baiting attacks: Malvertising: Fake online ads that spread malware, often disguised as legitimate promotions or software updates. Spear baiting: Targeted attacks to lure specific individuals or organizations with customized offers or files. Physical baiting: Infected physical media, like USB drives, left in public places or other areas where curious individuals might be tempted to pick them up and plug them into their devices. Cybersecurity tip: If something sounds too good to be true, it probably is. Be cautious of deals or offers that seem overly generous, especially from unfamiliar sources. 3. Diversion theft Diversion theft is a type of social engineering scheme where criminals trick couriers or delivery services into sending packages to the wrong person or place. They do this by impersonating someone from the delivery company, or the recipient, and convincing the target to change or confirm the wrong details. Cybersecurity tip: If you get an email or text message about a package delivery containing links or asking for additional information, double-check that the order number matches the one in the confirmation email you received when you first purchased the item. 4. Catfishing In catfishing scams, fraudsters create fake profiles on social media or dating platforms to trick people into sending them money or personal information. They often use attractive photos and send messages claiming they want a genuine relationship. Once the scammer forms a bond, they may ask for money to cover travel expenses or bring up some heartwrenching story like having a sick family member with unpaid medical bills. In other cases, they send malicious links to infect the victim's device with malware. Catfishers often request payment in the form of gift cards, since they're hard to trace. One distressing example of a catfishing scam is the "Keanu Reeves Scam." A Colorado woman was tricked into believing she was romantically involved with the actor, sending over $5,000 in gift cards after the scammer showed her fake documents and promised lavish trips. Despite the actor's representatives confirming he has no social media, she still believes it was the real Keanu Reeves. Cybersecurity tip: A red flag that you may be dealing with a catfisher is if the individual refuses to connect with you via video chat or meet in person. Another warning sign is if they invent a sob story to try to convince you to send them money or gift cards. 5. Pretexting Pretexting is a social engineering tactic in which a scammer impersonates a trusted source, such as your boss or a recruiter, to create a fake scenario and gain access to personal information. For example, in a job scam, a cybercriminal might notice that you're "open to work" on LinkedIn and pose as a representative of a company that matches your profile. They may inform you that you've been hired, but they need your Social Security number before you can start. Once you provide your personal information, the supposed company representative disappears. Cybersecurity tip: Legitimate employers will almost certainly never offer you a job without an interview. If you receive a suspicious job offer, contact the company directly through their official website to verify its authenticity. 6. Scareware Scareware is a type of social engineering scam that uses fear to trick people into downloading malware, sending money, or giving away personal information. It often starts with a pop-up message or phishing email claiming a virus has been detected on your device. The message then urges you to download (fake) antivirus software or pay a fee to fix a non-existent issue. In many cases, the software steals your information or infects your device with malware. Be cautious of any pop-ups from antivirus software not installed on your device as they're most likely a scam. A legitimate antivirus will notify you of issues within their app, not through pop-ups in a browser. Cybersecurity tip: Investing in real anti-virus software can help prevent malicious pop-ups, reducing your risk of falling for a scareware scam. 7. Watering hole In watering hole attacks, cybercriminals target websites frequently visited by a specific group, like employees of a company, to infect their devices with malware or steal sensitive data. The attackers compromise the website by embedding malicious code, which then infects visitors' devices. A watering hole attack can also use spoofed websites that mimic trusted ones. One real-life example of a watering hole attack occurred between November 2023 and July 2024, when the Russian-linked APT29 group compromised Mongolian government websites. The attackers injected malicious code into these sites, exploiting vulnerabilities in Apple iOS and Google Android. Their campaign specifically targeted unpatched devices, allowing the scammers to steal sensitive information from visitors. Cybersecurity tip: Avoid using company devices for personal activities. Only visit trusted websites related to work, and don't browse unfamiliar sites on work devices. Always check a website's URL carefully because a spoofed site can look very similar. 8. Quid pro quo A quid pro quo attack is a social engineering scam where the attacker offers something in exchange for sensitive information or access to a system. For example, the attacker might pose as a technical support agent, in return for the victim providing login credentials or other personal information. The goal is to exploit the target's willingness to accept help or reciprocate, so the social engineer gains unauthorized access or valuable information. Cybersecurity tip: Be cautious of unsolicited offers, especially if they require you to provide personal information or access to your accounts or device in exchange for help. 9. AI deepfakes AI deepfake scams use artificial intelligence to create fake videos and audio recordings of real people. Once the AI has enough data from video and audio recordings, it can generate highly realistic videos and voice clips in which people appear to say or do things they never actually did. Scammers use these AI scams to manipulate victims into taking actions like donating money, sharing sensitive information, or clicking malicious links. In one example, the British engineering firm Arup lost $25 million after scammers used AI-generated deepfake messages to impersonate the company's CFO. The scammer arranged a video call with an employee, convincing them to transfer large sums of money to bank accounts in Hong Kong. The fraud wasn't discovered until after the transactions were completed, underlining the significant threat of deepfake scams in business environments. Cybersecurity tip: Always be skeptical of videos and voice clips where a colleague or celebrity makes an unusual request. Contact your colleague via a different channel or look up a celebrity's official social page or website if you're planning on donating money. How to spot social engineering attacks Although cybercriminals are skilled at hiding their true intentions, most scams share a few common traits that make them easy to spot. Keep your eyes peeled for the following signs of a social engineering attack. Poor spelling and grammar: Many social engineering attacks, especially phishing emails, contain spelling or grammatical mistakes. In some cases, these are intentional — they allow the scammers to filter out recipients who are on the lookout for scams. Sense of urgency: Scammers often create a false sense of urgency, pressuring you to act quickly without thinking. They use phrases like "act now" or "limited time only" to manipulate you into making hasty decisions. Too-good-to-be-true promises: If an offer seems too good to be true, it likely is. Scammers often promise large sums of money, unexpected prizes, or amazing deals to lure you into providing personal information or downloading malware. Unsolicited contact: Receiving unsolicited messages, especially from unknown sources, should raise a red flag. Whether it's an email, phone call, text, or social media message, it could be a scam attempt if you didn't initiate contact. Unusual attachments or links: Be wary of emails or messages containing suspicious attachments or links. These could spread malware or steal your information, especially if the sender is someone you don't know or trust. What should I do if I'm the victim of a social engineering attack? If you fall for a social engineering attack, take the following steps to protect your personal information: Change your passwords on any compromised accounts and make sure they're strong and unique. Freeze your credit or set a fraud alert with the credit bureaus. Monitor your financial accounts for suspicious activity and contact your bank or card issuer if anything appears on your transactions. Report the incident to the FTC and you'll receive steps on how to protect yourself. Invest in identity theft protection to help monitor your credit and personal information online, and provide support if your identity is stolen in the future. Stay safer with LifeLock Awareness of common social engineering schemes can help protect you, but scammers will never stop trying to get their hands on your information. For additional security, subscribe to LifeLock Standard. Our robust identity-protection suite includes powerful features like Privacy Monitor, which helps reduce the public exposure of your personal information, and Dark Web Monitoring, which patrols the murkier corners of the internet and notifies you if it finds your information has been exposed. And if you do fall for a scam, our U.S.-based Personal Restoration Specialists can help you restore your identity and potentially reimburse you up to $25,000. FAQs What is the most common form of social engineering? Phishing attacks are the most common type of social engineering. Nearly nine million phishing attacks were detected around the world in 2023. What is the difference between phishing and social engineering? Social engineering is a broad term that refers to the practice of manipulating or deceiving individuals into disclosing confidential data or performing actions that benefit the attacker. Phishing, a narrower term, is a type of social engineering where cybercriminals request sensitive data or send dangerous links disguised as legitimate messages, often via email. What is a social engineer? A social engineer is someone who manipulates people into revealing confidential information or performing actions that compromise security, often by exploiting trust, emotions, or social norms. Can social engineering attacks happen offline, too? Yes, social engineering attacks can happen offline. For example, a scammer might gain physical access to a workplace by convincing a security guard that they "left their badge at home" or simply tailgating an employee through security doors. * Reimbursement and expense compensation varies according to plan. See policy terms, conditions, and exclusions at: GenDigital.com/legal. Stolen funds resulting from reasons other than identity theft, including voluntary transfers to scammers or disclosure of account data, are not eligible for reimbursement. More details here. Social engineering attacks come in many forms.getty In recent years, and particularly with the rise in use of social media, cyber criminals have taken to using psychological as well as technical methods of attack. Human beings, after all, are notoriously trusting, especially when distracted or under pressure. Hackers are increasingly exploiting this natural tendency in order to persuade their victims to reveal personal data or business secrets through psychological manipulation, in what's known as social engineering. Indeed, most cyber attacks these days are initiated in this way. Here are some of the more common types of social engineering attacks, and how they can best be avoided. Social engineering is a form of cyber attack in which criminals manipulate victims into handing over sensitive information. It is one of the biggest headaches for cybersecurity professionals these days. Typically, an attacker will first try to fool their victim into believing that they're trustworthy, often using information garnered from social media, before persuading them to hand over data or carry out actions to compromise security. Sometimes, these criminals are trying to fool individuals into parting with cash or personal data; sometimes they're attempting to steal corporate data in financially-motivated attacks. Sometimes, they're sponsored by antagonistic nation states and are trying to bring down critical infrastructure or persuade political figures to reveal secrets. Either way, it can lead to significant losses, with IBM's 2023 Cost of a Data Breach report finding that the average cost of a social engineering attack is $4.76 million. While the term social engineering covers any type of psychological trickery designed to elicit money or personal data, attacks tend to fall into one of several patterns. The most common types of attack include phishing, tailgating, pretexting, baiting and scareware (see below). With the exception of tailgating, they all depend on electronic means of communication, from phone calls and SMS to email and video. New technologies are making all these methods more convincing, with AI increasingly being used to craft more convincing communications; social media, meanwhile, can give attackers all the personal data they need to make their approach seem legitimate. Phishing is by far the commonest type of social engineering — and it's a growing trend, with Vade researchers finding that the number of attacks rose by 173% during the third quarter of 2023. Avoid the bait. getty Phishing involves contacting a victim via email, text (known as smishing) or a phone call (vishing) and using psychological techniques to trick them into revealing personal information or corporate data, or downloading malware. This usually means impersonating a business contact, a trusted institution such as a bank or even a family member, with attackers exploiting information they already have to make their lies more convincing. In one example, a Russian group known as Star Blizzard was found to be targeting defense and industrial organizations in the U.S. and U.K., impersonating known contacts of the target to persuade them to download a fraudulent link. While all phishing attacks are a form of social engineering, the two terms aren't quite synonymous, as social engineering can also happen in person rather than electronically. Tailgating Not all social engineering attacks take place online: sometimes, they're carried out in the real world. Tailgating is the art of gaining entrance to a physical location to steal information or otherwise do harm. This is a particular risk at busy workplaces — for example those that have large numbers of employees checking in and out, or those that have frequent deliveries or visits from subcontractors. Criminals will attempt to slip through a door behind a legitimate visitor, perhaps with their hands full so that the person in front holds the door open for them. Other methods include posing as a courier or delivery driver, or claiming to have lost their ID or forgotten an access code. Pretexting Pretexting is the process of softening a victim up by the creation of a plausible story, and forms the central plank of any social engineering attack. A cyber criminal may pose as a trustworthy person or organization — a boss, coworker or bank, for example — before setting up a particular scenario. Common examples include situations in which the victim is asked for urgent help, such as wiring money to a relative or boss. Other pretexting scams include emails offering lottery wins, cryptocurrency investments — or, in the case of romance scams, the love of the victim's life. In many cases, the scammer spends significant time and effort setting up the fake scenario. Baiting Baiting is just what it sounds like: the creation of an incentive to encourage the victim to take the hook. This could be a freebie, such as a prize or free movie, promised via a link to a malicious website. Sometimes, the bait is physical, such as a USB stick left lying around, perhaps labeled with something intriguing such as 'Confidential information' or 'Layoffs'. This was the attack method used by a China-linked hacker group called UNC53, discovered by security firm Mandiant in 2023: USB sticks left lying around in locations such as airport cafes and printing service shops were used to target more than 180 organizations in the U.S, Europe and Asia and deliver malware. Scareware While baiting techniques tempt a victim in, scareware does the same thing by putting the pressure on. One common tactic is the pop-up ad claiming that the victim has malware on their computer, and urging them to install new security software.Scareware is aptly named.getty Scareware always has an element of urgency about it, with the victim encouraged to believe that disaster will soon strike if they don't take immediate action. The fake ads are often extremely convincing, appearing to come from genuine antivirus suppliers, for example. In one recent example, Unit 42 researchers discovered a large-scale campaign dubbed ApateWeb that used a network of over 130,000 domains to deliver scareware, potentially unwanted programs and other scam pages. Real-World Social Engineering Examples In February 2024, personal finance journalist Charlotte Cowles revealed how she'd been persuaded to hand over $50,000 in cash after a complex social engineering scam — showing that anyone can fall victim. The elaborate scheme that fooled her involved a fake FTC investigator, a fake CIA agent and a highly detailed backstory. She lost $50,000 as a result. And in another example, the accounts of 27 cloud customers of software development company Retool had their accounts compromised after an attacker posed as a member of the IT team, and told recipients to click on a link to address a payroll-related issue. The social engineering began with an SMS message, but went on to involve a deepfake of the IT worker's voice. The crypto industry, meanwhile, is a frequent target for social engineering attacks, with a recent report from blockchain analysis firm Chainalysis recently finding that phishing scams have been used to steal $1 billion worth of cryptocurrencies since May 2021. In one example, a crypto trader reportedly lost $5.1 million in Beam tokens after suffering a phishing attack. How To Prevent Social Engineering Attacks Avoiding social engineering attacks essentially means being very, very suspicious. Individuals, whether at work or off-duty, should avoid opening unexpected emails without checking the source, or popping random USB sticks into their PC. They should beware of any approach pitched as being very urgent, use a good spam filter and keep anti-malware and anti-virus software up to date. Unique passwords should be used for each account, along with two-factor authentication. Organizations, meanwhile, should train people to this effect, and also introduce simple reporting mechanisms for employees who believe something may be amiss. And if the worst happens, passwords should be immediately changed, and a report filed with law enforcement or other relevant national bodies. Bottom Line Human beings are gullible, and can often be the weakest link in a company's cybersecurity strategy. A bit of healthy scepticism, staff training and basic security protections can help individuals and organizations minimize the risk. Social Engineering is an umbrella term for multiple malicious activities done by cyber criminals over the internet through human interaction. It doesn't involve the use of technical hacking techniques. Attackers use psychology and manipulation to trick users into performing actions that could compromise with their security including downloading malicious files, revealing sensitive information, clicking on malicious links, make transactions to illegal sources etc. It includes range of attacks including Phishing, Baiting, Tailagting, Pretexting, Scareware etc. as they all exploit the human trust. Social engineering is often the first step of larger cyber attacks. Purpose of Social Engineering AttacksThe purpose of social engineering attacks is typically to steal sensitive information, such as login credentials, credit card numbers, or personal information. Attackers can use this information for identity theft, financial fraud, or other malicious purposes. Another purpose of social engineering attacks is to gain unauthorized access to secure areas or systems.How do Social Engineering Attack Works? While social engineering attacks don't follow a fixed strategy, as attackers often adapt their tactics based on the victim, situation, and context, there are certain common elements that most social engineers employ. These key factors include:1. Planning and ResearchBefore launching a social engineering attack, the attacker spends time gathering information. This phase is critical to the success of the attack. The attacker may collect publicly available information about the target through:Social Media: Platforms like LinkedIn, Facebook, or Twitter can reveal personal details, job roles, contacts, and interests.Company Websites: Details about employees, company structure, and operational processes can be found here.Public Records: Information like employee directories, email addresses, and phone numbers can be found on company websites or government databases.This information helps the attacker craft a believable and tailored message, increasing the likelihood of success.2. Creating a Convincing PretextThe attacker develops a pretext, story designed to gain the trust of the victim. For example:Impersonation: The attacker might pose as a company executive, technical support, or a trusted colleague to ask for sensitive information or access.Urgency or Pressure: The attacker may create a sense of urgency to pressure the victim into acting quickly, such as claiming that immediate action is needed to fix a system issue or resolve an account problem.Familiarity: Attackers often use personal information about the target to make their approach seem more genuine (e.g., referencing the target's recent social media posts or common connections).The goal is to exploit the victim's natural tendency to trust familiar sources, especially in a work or personal context.3. Engaging with the VictimAfter the pretext is established, the attacker engages with the victim. The attack may take different forms:Phishing Emails: The attacker sends an email that appears legitimate, asking the victim to click on a malicious link or open an infected attachment. The email often includes a request for login credentials, sensitive data, or other confidential information.Phone Calls (Vishing): The attacker calls the victim, pretending to be from IT support or a trusted institution, and asks the victim to provide personal or financial information.SMS Messages (Smishing): The attacker sends a text message that mimics a legitimate service, prompting the victim to click on a malicious link or provide confidential information.4. Exploiting the TrustOnce the victim responds, the attacker exploits the trust established through the pretext. This could involve:Stealing Information: The attacker may gather sensitive data like login credentials, financial information, or personal identifiers.Gaining Unauthorized Access: The attacker may trick the victim into granting access to critical systems, networks, or databases, either by clicking on a link, downloading malware, or entering login credentials.Installing Malware: In some cases, the attacker may convince the victim to download malware disguised as legitimate software or documents, which could then be used to access the victim's system or data remotely.After successfully obtaining the desired information or access, the attacker can:Perform Financial Fraud: Using stolen credentials or sensitive data, the attacker can make unauthorized financial transactions.Access Sensitive Systems: The attacker may now have the ability to breach more secure areas of the organization, often leveraging compromised accounts to move laterally through the network.Install Ransomware: If the attacker has gained access to critical systems, they may deploy ransomware to demand payment for decryption.Sell Stolen Data: The attacker may sell sensitive information, such as personal records, intellectual property, or financial data, on the dark web.6. Covering Their TracksSocial engineers are often skilled at erasing signs of their presence. After exploiting the victim, they may:Delete or Modify Logs: Attackers may delete communication logs or traces of malware to avoid detection.Use Encryption: The attacker may encrypt sensitive data to prevent the victim from accessing it or identifying the breach.This stage ensures the attacker remains undetected for a longer period, allowing them to continue exploiting the situation or sell the data they have stolen.Types of Social Engineering There are many different types of social engineering attacks, each of which uses a unique approach to exploit human weaknesses and gain access to sensitive information. Here are some of the types of attacks, include:1. PhishingPhishing is a type of social engineering attack that involves sending an email or message that appears to be from a legitimate source, such as a bank, in an attempt to trick the recipient into revealing their login credentials or other sensitive information.2. BaitingBaiting is a type of social engineering attack that involves leaving a tempting item, such as a USB drive, in a public place in the hope that someone will pick it up and plug it into their computer. The USB drive is then used to infect the computer with malware.3. TailgatingTailgating is a type of social engineering attack that involves following an authorized individual into a secure area, such as a building or data center, without proper authorization.4. PretextingPretexting is a type of social engineering attack that involves creating a false identity or situation in order to trick an individual into revealing sensitive information. For example, an attacker might pretend to be a customer service representative in order to trick an individual into giving them their login credentials.5. ScarewareScareware is when the victim is sent false messages claiming their system is infected with a malware, or outdated, suggesting them to download softwares to resolve the issue. Downloading the software would lead to the attackers gaining access to the system.Prevention against Social Engineering AttacksSocial engineering attacks rely on manipulating human psychology rather than exploiting technical vulnerabilities, making it important for individuals to remain vigilant and proactive. Below are some strategies to adopt by an individual to prevent from falling victim to these attacks:1. Avoid Opening Emails and Attachments from Suspicious SourcesPhishing emails often appear legitimate but contain malicious links or attachments designed to steal personal information or install malware. Always be cautious when receiving unsolicited emails, especially those requesting sensitive data or action.Check the sender's email address carefully.Avoid clicking on suspicious links or downloading attachments.Verify requests through alternative channels (e.g., by calling or messaging the official number).2. Enable Multi-Factor Authentication (MFA)Multi-factor authentication (MFA) adds an extra layer of security by requiring more than just a password. This reduces the risk of unauthorized access, even if your password is compromised.Enable MFA for critical accounts (e.g., email, banking, social media).Use authentication apps like Google Authenticator for added security.Enable biometric authentication where possible.3. Beware of Tempting BaitsCyber attackers often use enticing offers to lure victims into clicking malicious links or downloading infected files. Be cautious of "too good to be true" deals.Be wary of unsolicited offers, discounts, or free downloads.Avoid clicking on unknown links or downloading files from unfamiliar sources.Always verify the legitimacy of offers before acting.Impact Of Social Engineering Attack On OrganizationSocial engineering attacks can have severe consequences for organizations, as they exploit human behavior and manipulate individuals into divulging sensitive information or performing actions that compromise security. The impact of a successful social engineering attack can range from financial losses and data breaches to long-term reputational damage. This losses include:1. Financial LossesCompetitors may utilize social engineering procedures to take touchy data, for example, advancement plans and advertising systems of an objective organization, which can result in a financial misfortune to the objective organization.2. Harm to GoodwillFor an association, altruism is significant for drawing in clients. Social engineering assaults may harm that altruism by releasing touchy hierarchical information.3. Loss of PrivacyPrivacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and may discontinue the business association with the organization. Consequently, the organization could face losses.4. Dangers of TerrorismTerrorism and anti-social elements pose a threat to an organization's assets- people and property. Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets.5. Lawsuits and ArbitrationLawsuits and arbitration result in negative publicity for an organization and affects the business's performance.6. Temporary or Permanent ClosureSocial engineering attacks can result in a loss of goodwill. Lawsuits and arbitration may force a temporary or permanent closure of an organization and its business activities.ConclusionSocial engineering attacks are one of the most dangerous cyber threats, as they target human psychology rather than technical vulnerabilities. Attackers manipulate individuals into performing actions that compromise security, such as revealing sensitive information, downloading malware, or granting unauthorized access. These attacks, including phishing, baiting, and pretexting, are often the first step in more extensive cyber attacks, making them particularly harmful.The impact of a successful social engineering attack on an organization could lead to financial losses, harm to reputation, legal issues, and even the potential closure of the business. Protecting against such attacks requires a proactive approach, including being cautious of suspicious communications, enabling multi-factor authentication, and staying vigilant about tempting offers. Cyber Security Tutorial OSI Security Architecture Active and Passive attacks in Information Security Types of Security Mechanism A Model for Network Security Basics of Wi-Fi The Internet and the Web What is a Website ? Cryptography and Network Security Principles Public Key Infrastructure What is Electronic Signature? Identity and Access Management What Is Cloud Computing ? Types, Architecture, Examples and Benefits Cyber Crime Cyber Criminals and their types Psychological Profiling in Cybersecurity What is Social Engineering? Working, Types, Prevention and Impact Cyberstalking How to Defend Against Botnets ? Emerging Attack Vectors in Cyber Security What is Malware? And its Types What is Phishing? Cyber Crime - Identity Theft What is Cyber Terrorism? Worms, Viruses and beyond !! What is a Trojan Horse? Definition, Examples and More Image Steganography in Cryptography Difference between DOS and DDOS attack Types of SQL Injection (SQLi) Buffer Overflow Attack with Example Reverse Engineering - Software Engineering Difference Between Vulnerability and Exploit Basic Network Attacks in Computer Network Kali Linux - Hacking Wi-Fi Web Server and its Types of Attacks Types of VoIP Hacking and Countermeasures How to Spoof SMS Message in Linux ? Difference Between Backup and Recovery Manual Code Review : Security Assessment Penetration Testing - Software Engineering Security Testing Tools - Software Testing Intrusion Detection System (IDS) What is Vulnerability Assessment? Secure coding - What is it all about? Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password. Famous hacker Kevin Mitnick helped popularize the term 'social engineering' in the '90s, although the idea and many of the techniques have been around as long as there have been scam artists. Even if you've got all the bells and whistles when it comes to securing your data center, your cloud deployments, your building's physical security, and you've invested in defensive technologies, have the right security policies and processes in place and measure their effectiveness and continuously improve, still a crafty social engineer can weasel his way right through (or around). The phrase "social engineering" encompasses a wide range of behaviors, and what they all have in common is that they exploit certain universal human qualities: greed, curiosity, politeness, deference to authority, and so on. While some classic examples of social engineering take place in the "real world"—a man in a FedEx uniform bluffing his way into an office building, for example—much of our daily social interaction takes place online, and that's where most social engineering attacks happen as well. For instance, you might not think of phishing or smishing as types of social engineering attacks, but both rely on tricking you—by pretending to be someone you trust or tempting you with something you want—into downloading malware onto your device. This brings up another important point, which is that social engineering can represent a single step in a larger attack chain. A smishing text uses social dynamics to entice you with a free gift card, but once you tap the link and download malicious code, your attackers will be using their technical skills to gain control of your device and exploit it. A good way to get a sense of what social engineering tactics you should look out for is to know about what's been used in the past. We've got all the details in an extensive article on famous social engineering attacks, but for the moment let's focus on three social engineering techniques — independent of technological platforms — that have been successful for scammers in a big way. Offer something sweet. As any con artist will tell you, the easiest way to scam a mark is to exploit their own greed. This is the foundation of the classic Nigerian 419 scam, in which the scammer tries to convince the victim to help get supposedly ill-gotten cash out of their own country into a safe bank, offering a portion of the funds in exchange. These "Nigerian prince" emails have been a running joke for decades, but they're still an effective social engineering technique that people fall for: in 2007 the treasurer of a sparsely populated Michigan county gave $1.2 million in public funds to such a scammer in the hopes of personally cashing in. Another common lure is the prospect of a new, better job, which apparently is something far too many of us want: in a hugely embarrassing 2011 breach, the security company RSA was compromised when at least two low-level employees opened a malware file attached to a phishing email with the file name "2011 recruitment plan.xls." Fake it till you make it. One of the simplest — and surprisingly most successful — social engineering techniques is to simply pretend to be your victim. In one of Kevin Mitnick's legendary early scams, he got access to Digital Equipment Corporation's OS development servers simply by calling the company, claiming to be one of their lead developers, and saying he was having trouble logging in; he was immediately rewarded with a new login and password. This all happened in 1979, and you'd think things would've improved since then, but you'd be wrong: in 2016, a hacker got control of a U.S. Department of Justice email address and used it to impersonate an employee, coaxing a help desk into handing over an access token for the DoJ intranet by saying it was his first week on the job and he didn't know how anything worked. Many organizations do have barriers meant to prevent these kinds of brazen impersonations, but they can often be circumvented fairly easily. When Hewlett-Packard hired private investigators to find out which HP board members were leaking info to the press in 2005, they were able to supply the PIs with the last four digits of their targets' social security number — which AT&T's tech support accepted as proof of ID before handing over detailed call logs. Act like you're in charge. Most of us are primed to respect authority — or, as it turns out, to respect people who act like they have the authority to do what they're doing. You can exploit varying degrees of knowledge of a company's internal processes to convince people that you have the right to be places or see things that you shouldn't, or that a communication coming from you is really coming from someone they respect. For instance, in 2015 finance employees at Ubiquiti Networks wired millions of dollars in company money to scam artists who were impersonating company executives, probably using a lookalike URL in their email address. On the lower tech side, investigators working for British tabloids in the late '00s and early '10s often found ways to get access to victims' voicemail accounts by pretending to be other employees of the phone company via sheer bluffing; for instance, one PI convinced Vodafone to reset actress Sienna Miller's voicemail PIN by calling and claiming to be "John from credit control." Sometimes it's external authorities whose demands we comply with without giving it much thought. Hillary Clinton campaign honcho John Podesta had his email hacked by Russian spies in 2016 when they sent him a phishing email disguised as a note from Google asking him to reset his password. By taking action that he thought would secure his account, he actually gave his login credentials away. Phishing, as we noted above, which also includes text-based smishing and voice-based vishing These attacks are often low-effort but widely spread; for instance, a phisher might send out thousands of identical emails, hoping someone will be gullible enough to click on the attachment. Spear phishing, or whaling, is a "high-touch" variation of phishing for high-value targets. Attackers spend time researching their victim, who's usually a high-status person with a lot of money they can be separated from, in order to craft unique and personalized scam communications. Baiting is a key part of all forms of phishing and other scams as well—there's always something to tempt the victim, whether a text with a promise of a free gift card or something much more lucrative or salacious. Pretexting involves creating a story, or pretext, to convince someone to give up valuable information or access to some system or account. A pretexter might manage to find some of your personally identifying information and use it to trick you—for instance, if they know what bank you use, they might call you up and claim to be a customer service rep who needs to know your account number to help with a late payment. Or they could use the information to imitate you—this was the technique used by those HP PIs we discussed above. Business email compromise (BEC), also known as CEO fraud, combines several of the above techniques. An attacker either gains control of a victim's email address or manages to send emails that look like they're from that address, then start sending emails to subordinates at work requesting the transfer of funds to accounts they control. [Related reading: Israeli threat group uses fake company acquisitions in CEO fraud schemes] In a quid pro quo attack, a hacker offers something in exchange for access or information. A tech support scam is a typical example of a quid pro quo attack. Tailgating is an in-real-life form of social engineering in which an attacker tricks an employee into following them into the building, hence 'tailgating.' This is achieved, for example by pretending to be a delivery person or pretending to be an employee who forgot their badge and takes advantage of the human desire to be helpful and nice. The security company Norton has done a pretty good job of outlining some red flags that could be a sign of a social engineering attack. These apply across social and technological techniques, and are good to keep in the back of your mind as you try to stay on guard: Someone you know sends an unusual message: Stealing or mimicking someone's online identity and then mining their social circles is relatively easy for a determined attacker, so if you get a message from a friend, relative, or coworker that seems off, be very sure you're really talking to them before you act on it. It's possible that your granddaughter really is on a vacation she didn't tell you about and needs money, or that your boss really does wants you to wire a six-figure sum to a new supplier in Belarus, but that's something for you to triple-check before you hit send. A stranger is making an offer that's too good to be true: Again, we all laugh at the Nigerian prince emails, but many of us still fall for scams that trick us by telling us we're about to get something we never expected and never asked for. Whether it's an email telling you won a lottery you didn't enter or a text from a weird number offering you a free gift card just for paying your phone bill on time, if it feels too good to be true, it probably is. Your emotions are heightened and you have to act now: Social engineering scammers play on strong emotions—fear, greed, empathy—to inculcate a sense of urgency specifically so you don't stop to think twice about scenarios like the ones we just outlined. A particularly pernicious technique in this realm is a tech support scam, which preys on people who are already nervous about hacks but not very tech savvy: you hear from an aggressive person who claims to be from Google or Microsoft, tells you that your system has been compromised, and demands that you change your passwords right away—tricking you into revealing your credentials to them in the process. Fighting against all of these techniques requires vigilance and a zero-trust mindset. That can be difficult to inculcate in ordinary people; in the corporate world, security awareness training is the number one way to prevent employees from falling prey to high-stakes attacks. Employees should be aware that social engineering exists and be familiar with the most commonly used tactics. Some basic tips to avoid falling victim to social engineering attacks include: Resist the urge to click links in a suspicious email. Check the Web address of a link (by placing your mouse cursor over the link) and the sender's email address before visiting the destination website. Visit websites directly rather than clicking links in emails. Be cautious of email attachments, even if it looks like it's from a familiar sender. Check for signs such as poor quality of the logo or email, poor grammar or misspellings. Fortunately, social engineering awareness lends itself to storytelling. And stories are much easier to understand and much more interesting than explanations of technical flaws. Quizzes and attention-grabbing or humorous posters are also effective reminders about not assuming everyone is who they say they are. But it isn't just the average employee who needs to be aware of social engineering. As we saw, social engineers focus on high-value targets like CEOs and CFOs. Senior leadership often resists going to the trainings mandated for their employees, but they need to be aware of these attacks more than anyone. CSO contributor Dan Lohrmann offers the following advice: Train and train again when it comes to security awareness.Ensure that you have a comprehensive security awareness training program in place that is regularly updated to address both the general phishing threats and the new targeted cyberthreats. Remember, this is not just about clicking on links. Provide a detailed briefing "roadshow" on the latest online fraud techniques to key staff.Yes, include senior executives, but don't forget anyone who has authority to make wire transfers or other financial transactions. Remember that many of the true stories involving fraud occur with lower-level staff who get fooled into believing an executive is asking them to conduct an urgent action — usually bypassing normal procedures and/or controls. Review existing processes, procedures, and separation of duties for financial transfers and other important transactions.Add extra controls, if needed. Remember that separation of duties and other protections may be compromised at some point by insider threats, so risk reviews may need to be reanalyzed given the increased threats. Consider new policies related to "out of band" transactions or urgent executive requests.An email from the CEO's Gmail account should automatically raise a red flag to staff, but they need to understand the latest techniques being deployed by the dark side. You need authorized emergency procedures that are well-understood by all. Review, refine and test your incident management and phishing reporting systems.Run a tabletop exercise with management and with key personnel on a regular basis. Test controls and reverse-engineer potential areas of vulnerability. 50%Business email compromise (BEC) attacks comprise 50% of all social engineering (source: Verizon's DBIR for 2023). A number of vendors offer tools or services to help conduct social engineering exercises, and/or to build employee awareness via means such as posters and newsletters. Also worth checking out is social-engineer.org's Social Engineering Toolkit, which is a free download. The toolkit helps automate penetration testing via social engineering, including spear phishing attacks, creation of legitimate-looking websites, USB drive-based attacks, and more. Another good resource is The Social Engineering Framework. Currently, the best defense against social engineering attacks is user education and layers of technological defenses to better detect and respond to attacks. Detection of key words in emails or phone calls can be used to weed out potential attacks, but even those technologies will probably be ineffective in stopping skilled social engineers. Frank Abagnale is probably the most famous example of a social engineering attack. The book and movie Catch Me if You Can depict how Mr. Abagnale impersonated several people, including a doctor, a lawyer, and an airplane pilot to gain people's trust and take advantage of them. In 2011, an attacker penetrated the security company RSA by sending phishing emails to groups of employees. The emails had an Excel spreadsheet attached. The spreadsheet had malicious code embedded in it, which used a vulnerability in Adobe Flash to install a backdoor into the system. If the employees had not been socially engineered into opening the file, the attack would not have been successful. Phishing in a pandemic is also common, so users should always be on the lookout. To spot a social engineering attack, look for the following signs: An emotional plea that leverages fear, curiosity, excitement, anger, sadness, or guilt A sense of urgency around the request An attempt to establish trust with the recipient In short, anytime someone tries to get you to provide money or sensitive information through manipulation or coercion, you are being targeted with a social engineering attack. Always be careful when communicating online, and never trust anyone whose identity you cannot confirm. Most importantly, never click on anything that looks suspicious, and never divulge sensitive information. Instead of clicking on a Uniform Resource Locator (URL), type it in manually in the address bar. Double-check the origin of all URLs before clicking on them, and if you cannot verify their legitimacy, avoid them. Using more than a password to access an account can help prevent social engineers from breaching a system. This could include biometrics or temporary passwords sent through a text message. Your passwords should be both complex and unique, never repeated for more than one site or account. You can use a secure password manager to organize them and have them available when needed. A relationship that does not include any in-person interaction or phone conversation can easily be used for social engineering in 2021. Beware of anyone who wants to interact solely online. Allowing someone to access your primary Wi-Fi network leaves it open to eavesdropping. To prevent this, use a guest network for those who visit your office or home. A virtual private network (VPN) provides you with a secure, encrypted tunnel through which communications pass. Even if someone were to snoop on your communications, the VPN would encrypt the transmissions, rendering them useless for the attacker. While your Wi-Fi connections at and around the office are likely secured, as are your mobile devices, it is important to not neglect other devices such as infotainment systems in your car. Getting within these systems can help a social engineer further personalize their attack. Internet security software can protect your system from malware that gets implanted via a social engineering attack. Some security solutions can also track the source of the attack, which can be reported to authorities to aid in their investigation of the crime. Your computer and mobile devices should always be locked up or securely on your person. This holds true whether you are in a public place or a semi-public environment like your job. Software updates help ensure your applications are impervious to the newest kinds of attacks on the landscape. After an attack has been successful, the software's design team may address the vulnerability in an update, so frequent updates provide you with the most up-to-date security. Some companies keep track of accounts that have been compromised by hackers. If your account information is on their list, take steps to secure it by changing your password or adding MFA. Baiting is a type of social engineering attack wherein scammers make false promises to users in order to lure them into revealing personal information or installing malware on the system.Baiting scams can be in the form of tempting ads or online promotions, such as free game or movie downloads, music streaming or phone upgrades. The attacker hopes that the password the target uses to claim the offer is one they have also used on other sites, which can allow the hacker to access the victim's data or sell the information to other criminals on the dark web.Baiting can also be in a physical form, most commonly via a malware-infected flash drive. The attacker would leave the infected flash drive in an area where the victim is most likely to see it. This would prompt the victim to insert the flash drive into the computer to find out who it belongs to. In the meantime, malware is installed automatically.4. Diversion theftDiversion theft is a cyberattack that originated offline. In this attack, a thief persuades a courier to pick up or drop off a package in the wrong location, deliver an incorrect package or deliver a package to the wrong recipient.Diversion theft has since been adapted as an online scheme. The malicious actor steals confidential information by tricking the user into sending it to the wrong recipient.This attack type often involves spoofing, which is a technique used by cybercriminals to disguise themselves as a known or trusted source. Spoofing can take many forms, such as spoofed emails, IP spoofing, DNS Spoofing, GPS spoofing, website spoofing, and spoofed calls.5. Business email compromise (BEC)Business Email Compromise (BEC) is a social engineering tactic where the attacker poses as a trustworthy executive who is authorized to deal with financial matters within the organization.In this attack scenario, the scammer closely monitors the executive's behavior and uses spoofing to create a fake email account. Through impersonation, the attacker sends an email requesting their subordinates make wire transfers, change banking details and carry out other money-related tasks.BEC can result in huge financial losses for companies. Unlike other cyber scams, these attacks do not rely on malicious URLS or malware that can be caught by cybersecurity tools, like firewalls or endpoint detection and response (EDR) systems. Rather, BEC attacks are carried out strictly by personal behaviour, which is often harder to monitor and manage, especially in large organizations.6. Smishing / SMS-phishingSMS-phishing, or smishing, is a social engineering attack conducted specifically through SMS messages. In this attack, scammers attempt to lure the user into clicking on a link which directs them to a malicious site. Once on the site, the victim is then prompted to download malicious software and content.Smishing attacks have increased in popularity amongst criminals as people spend more time on mobile devices. While users have become savvier at detecting email phishing, many people are far less aware of the risks associated with text messages.A smishing attack requires little effort for threat actors and is often carried out by simply purchasing a spoofed number and setting up the malicious link.7. Quid pro quoA quid pro quo attack involves the attacker requesting sensitive information from the victim in exchange for a desirable service.For example, the attacker may pose as an IT support technician and call a computer user to address a common IT issue, such as slow network speeds or system patching to acquire the user's login credentials. Once the credentials are exchanged, this information is used to gain access to other sensitive data stored on the device and its applications, or it is sold on the dark web.8. PretextingPretexting is a form of social engineering that involves composing plausible scenarios, or pretext, that are likely to convince victims to share valuable and sensitive data.Pretexters may impersonate someone in a position of authority, such as a member of law enforcement or a tax official, or a person of interest, such as a talent agency scout or sweepstakes organizer. After explaining the context, the attacker would then ask the victim questions to gain personal and sensitive information, which they could then use to advance other attack scenarios or access their personal accounts.9. HoneytrapA honeytrap attack is a social engineering technique that specifically targets individuals looking for love on online dating websites or social media. The criminal befriends the victim by creating a fictional persona and setting up a fake online profile. Over time, the criminal takes advantage of the relationship and tricks the victim into giving them money, extracting personal information, or installing malware.10. Tailgating/PiggybackingTailgating, also known as piggybacking, is a physical breach whereby an attacker gains access to a physical facility by asking the person entering ahead of them to hold the door or grant them access. The attacker may impersonate a delivery driver or other plausible identity to increase their chances. Once inside the facility, the criminal can use their time to conduct reconnaissance, steal unattended devices or access confidential files.Tailgating can also include allowing an unauthorized person to borrow an employee's laptop or other device so that the user can install malware.How to prevent social engineering attacksWhile it is impossible to prevent social engineering attacks from taking place, people and organizations can protect themselves through responsible behavior, security awareness, education and vigilance.Here are some helpful considerations to reference when receiving any form of communication from an unknown, unfamiliar or suspicious source:Individual Users Social engineering is a technique used by cyber attackers to trick people into giving away sensitive information. Instead of hacking computers directly, attackers manipulate human behavior—making people the weakest link in security. It's not just about emails or phone calls; it's about psychological tricks. Attackers might act like trusted coworkers, IT staff, or even bank officials to steal your data, login credentials, or money. Why Is Social Engineering Dangerous? Social engineering is dangerous because: It's hard to detect—no malware or virus is needed. It works on emotions like fear, urgency, or trust. It targets humans, not systems, making it very effective. Even trained professionals can fall for it if they're not careful. Types of Social Engineering Attacks Let's look at the most common types of social engineering: Type What It Does Phishing Fake emails or websites asking for passwords or personal info. Vishing Phone calls pretending to be from tech support or banks. Smishing Text messages with harmful links or fake offers. Pretexting Creating a fake scenario to gain trust and extract info. Baiting Leaving infected USBs or links to tempt victims. Tailgating Following authorized personnel into secured areas without proper ID. Quid Pro Quo Offering something (like free software/help) in exchange for access or info. Real-World Example of Social Engineering Imagine someone calls your office pretending to be an IT technician. They say there's a virus spreading in the company and ask for your computer login details to fix it. Trusting them, you give the info—and now they have access to your system. That's social engineering in action. Why Social Engineering Works So Well Attackers exploit: Lack of awareness Emotional manipulation (fear, greed, curiosity) Overtrust in authority Lack of security training Many people assume threats only come from viruses or hackers, not from everyday conversations or emails. Impact of Social Engineering Attacks The consequences of falling for these attacks can be huge: Data theft (personal and business) Financial loss Reputation damage Legal consequences due to data breaches Network compromises that lead to larger attacks (like ransomware) Key Social Engineering Concepts You Should Know Here are important terms that will help you understand future parts of this series: Concept Description Psychological Manipulation Tricking someone using emotion, urgency, or authority. Threat Actor The person or group performing the attack. Attack Vector The path or method used to exploit the target (email, phone, USB, etc.). Payload The harmful content delivered (like a phishing link or malicious file). Human Attack Surface All ways people can be targeted and exploited for information. How to Identify a Social Engineering Attempt Watch for: Unusual requests for personal info Messages with poor grammar or spelling Urgent tone or threats ("Your account will be blocked in 10 mins!") Requests to click on strange links or open attachments Conclusion: Stay Alert, Stay Safe Social engineering is not a new threat, but it's getting smarter and harder to detect. By understanding the core concepts and how attackers operate, you're already one step ahead. In the next part, we'll dive deep into Human-Based Social Engineering Techniques, with real examples and how to defend against them. FAQs What is social engineering in cybersecurity? Social engineering is a tactic used by attackers to manipulate people into revealing sensitive data through psychological tricks rather than technical hacking. Why is social engineering effective? It targets human emotions like trust, fear, or urgency, making people act without thinking. What are the common types of social engineering attacks? Phishing, vishing, smishing, baiting, pretexting, tailgating, and quid pro quo are common types. How does phishing work in social engineering? Phishing uses fake emails or websites to trick users into providing passwords or personal information. What is vishing? Vishing is voice phishing—attackers call pretending to be from a trusted organization to steal information. What is smishing? Smishing is SMS-based phishing where attackers send texts with malicious links. What is pretexting in cybersecurity? Pretexting involves creating a fake story or scenario to gain someone's trust and extract data. How does baiting work in social engineering? Baiting uses tempting offers, like free software or USBs, to get users to download malware. What is tailgating in social engineering? Tailgating involves following someone into a secured building or area without authorization. What is quid pro quo attack? Attackers offer a service or help in exchange for login credentials or access. What are social engineering concepts? They include psychological manipulation, threat actors, attack vectors, and payloads. Why is phishing considered a form of social engineering? Because it uses human trust and urgency to manipulate victims into disclosing private data. What is a human attack surface? It refers to all possible ways a person can be manipulated to reveal sensitive information. What role does psychology play in social engineering? Attackers use emotions like fear, greed, or trust to influence victim behavior. Is social engineering illegal? Yes, it's a form of cybercrime when used to gain unauthorized access to information or systems. Can companies fall for social engineering attacks? Absolutely. Even large organizations are often victims of phishing or pretexting schemes. What is the impact of a successful social engineering attack? It can lead to data breaches, financial loss, reputational damage, and compromised systems. How can you detect a social engineering attempt? Look for urgent language, unknown links, and requests for personal or financial information. Are antivirus tools effective against social engineering? Not always. Since it targets human behavior, awareness training is more effective. What's the difference between social engineering and malware attacks? Social engineering manipulates people, while malware attacks exploit software vulnerabilities. How do attackers impersonate trusted brands? By creating fake websites, emails, or even phone scripts that mimic real organizations. What should you do if you suspect a social engineering attack? Don't respond, don't click any links, and report it to your security team or authority. Why do people fall for social engineering scams? Because attackers are convincing and use urgency, fear, or authority to pressure victims. What industries are most targeted by social engineering? Finance, healthcare, education, and government sectors are common targets. How often do social engineering attacks occur? They happen daily and are among the most common cybersecurity threats worldwide. Can social engineering lead to ransomware attacks? Yes, it often serves as the initial access point for delivering ransomware. What is the best defense against social engineering? Security awareness training, skepticism of unsolicited messages, and verifying all requests. Can AI help detect social engineering attacks? Yes, some tools use AI to identify phishing patterns and suspicious communication behavior. Is social engineering used in physical security breaches? Yes, attackers may gain access to restricted areas by impersonating staff or delivery workers. What is the first step to preventing social engineering? Education—understanding how these attacks work is the best defense. Social engineering attacks manipulate people into sharing information that they shouldn't share, downloading software that they shouldn't download, visiting websites they shouldn't visit, sending money to criminals or making other mistakes that compromise their personal or organizational security. An email that seems to be from a trusted coworker requesting sensitive information, a threatening voicemail claiming to be from the IRS and an offer of riches from a foreign potentate are just a few examples of social engineering. Because social engineering uses psychological manipulation and exploits human error or weakness rather than technical or digital system vulnerabilities, it is sometimes called "human hacking". Cybercriminals frequently use social engineering tactics to obtain personal data or financial information, including login credentials, credit card numbers, bank account numbers and Social Security numbers. They use the stolen information for identity theft, enabling them to make purchases using other peoples' money or credit, apply for loans in someone else's name, apply for other peoples' unemployment benefits and more. But a social engineering attack can also be the first stage of a larger-scale cyberattack. For example, a cybercriminal might trick a victim into sharing a username and password and then use those credentials to plant ransomware on the victim's employer's network. Social engineering is attractive to cybercriminals because it enables them to access digital networks, devices and accounts without having to do the difficult technical work of getting around firewalls, antivirus software and other cybersecurity controls. This is one reason why social engineering is the leading cause of network compromise today according to ISACAs State of Cybersecurity 2022 report. According to IBM's Cost of a Data Breach report, breaches caused by social engineering tactics (such as phishing and business email compromise) were among the most costly. Social engineering tactics and techniques are grounded in the science of human motivation. They manipulate victims' emotions and instincts in ways proven to drive people to take actions that are not in their best interests. Most social engineering attacks employ one or more of the following tactics: Posing as a trusted brand: Scammers often impersonate or "spoof" companies that victims know, trust and perhaps do business with often or regularly, so regularly that they follow instructions from these brands reflexively, without taking the proper precautions. Some social engineering scammers use widely available kits for staging fake websites that resemble those of major brands or companies. Posing as a government agency or authority figure: People trust, respect or fear authority (in varying degrees). Social engineering attacks play on these instincts with messages that appear or claim to be from government agencies (example: the FBI or IRS), political figures or even celebrities. Inducing fear or a sense of urgency: People tend to act rashly when scared or hurried. Social engineering scams can use any number of techniques to induce fear or urgency in victims. For instance, telling the victim that a recent credit transaction was not approved, that a virus has infected their computer, that an image used on their website violates a copyright and so on. Social engineering can also appeal to victims' fear of missing out (FOMO), which creates a different kind of urgency. Appealing to greed: The Nigerian Prince scam, an email wherein someone claiming to be a Nigerian royal trying to flee his country offers a giant financial reward in exchange for the recipient's bank account information or a small advance fee, is one of the best-known examples of social engineering that appeals to greed. This type of social engineering attack can also come from an alleged authority figure and creates a sense of urgency, which is a powerful combination. This scam is as old as email itself, but was still raking in USD 700,000 per year as of 2018. Appealing to helpfulness or curiosity: Social engineering ploys can also appeal to victims' better nature. For instance, a message that appears to be from a friend or a social networking site can offer technical help, ask for participation in a survey, claim that the recipients' post has gone viral and provide a spoofed link to a fake website or malware download. Phishing attacks are digital or voice messages that try to manipulate recipients into sharing sensitive information, downloading malicious software, transferring money or assets to the wrong people or taking some other damaging actions.

Scammers craft phishing messages to look or sound like they come from a trusted or credible organization or individual, sometimes, even an individual the recipient knows personally. There are many types of phishing scams: Bulk phishing emails are sent to millions of recipients at a time. They appear to be sent by a large, well-known business or organization, such as a national or global bank, a large online retailer, a popular online payments provider and so on. In these emails they make a generic request such as "we're having trouble processing your purchase, please update your credit information". Frequently, these messages include a malicious link that takes the recipient to a fake website that captures the recipient's username, password, credit card data and more. Spear phishing targets a specific individual, typically one with privileged access to user information, the computer network or corporate funds. A scammer researches the target, often using information that is found on LinkedIn, Facebook or other social media to create a message that appears to come from someone the target knows and trusts or that refers to situations with which the target is familiar. Whale phishing is a spear phishing attack that targets a high-profile individual, such as a CEO or political figure. In business email compromise (BEC), the hacker uses compromised credentials to send email messages from an authority figure's actual email account, making the scam that much more difficult to detect. Voice phishing or vishing, is phishing that is conducted through phone calls. Individuals typically experience vishing in the form of threatening recorded calls claiming to be from the FBI. SMS phishing, or smishing, is phishing through a text message. Search engine phishing involves hackers creating malicious websites that rank high in search results for popular search terms. Angler phishing is phishing using fake social media accounts that masquerade as the official accounts of trusted companies' customer service or customer support teams. According to the IBM® X-Force® Threat Intelligence Index, phishing is the leading malware infection vector, identified in 41% of all incidents. According to the Cost of a Data Breach report, phishing is the initial attack vector leading to the most costly data breaches. Baiting lures (no pun intended) victims into knowingly or unwittingly giving up sensitive information or downloading malicious code by tempting them with a valuable offer or even a valuable object. The Nigerian Prince scam is probably the best-known example of this social engineering technique. More current examples include free but malware-infected games, music or software downloads. But some forms of baiting are barely artful. For example, some threat actors leave malware-infected USB drives where people will find them, grab them and use them because "hey, free USB drive". In tailgating, also called "piggybacking", an unauthorized person closely follows an authorized person into an area containing sensitive information or valuable assets. Tailgating can be conducted in person, for example, a threat actor can follow an employee through an unlocked door. But tailgating can also be a digital tactic, such as when a person leaves a computer unattended while still logged in to a private account or network. In pretexting, the threat actor creates a fake situation for the victim, and poses as the right person to resolve it. Very often (and most ironically) the scammer claims that the victim has been impacted by a security breach, and then offers to fix things if the victim will provide important account information or control over the victim's computer or device. Technically speaking, almost every social engineering attack involves some degree of pretexting. In a quid pro quo scam, hackers dangle a desirable good or service in exchange for the victim's sensitive information. Fake contest winnings or seemingly innocent loyalty rewards ("thank you for your payment, we have a gift for you") are examples of quid pro quo ploys. Also considered a form of malware, scareware is software that uses fear to manipulate people into sharing confidential information or downloading malware. Scareware often takes the form of a fake law enforcement notice accusing the user of a crime, or a fake tech support message warning the user of malware on their device. From the phrase "somebody poisoned the watering hole", hackers inject malicious code into a legitimate web page that is frequented by their targets. Watering hole attacks are responsible for everything, from stolen credentials to unwitting drive-by ransomware downloads. Social engineering attacks are notoriously difficult to prevent because they rely on human psychology rather than technological pathways. The attack surface is also significant: In a larger organization, it takes just one employee's mistake to compromise the integrity of the entire enterprise network. Some of the steps that experts recommend to mitigate the risk and success of social engineering scams include: Security awareness training: Many users don't know how to identify social engineering attacks. In a time when users frequently trade personal information for goods and services, they don't realize that surrendering seemingly mundane information, such as a phone number or date of birth, can allow hackers to breach an account. Security awareness training, combined with data security policies, can help employees understand how to protect their sensitive data and how to detect and respond to social engineering attacks in progress. Access control policies: Secure access control policies and technologies, including multifactor authentication, adaptive authentication and a zero trust security approach can limit cybercriminals' access to sensitive information and assets on the corporate network even if they obtain users' login credentials. Cybersecurity technologies: Spam filters and secure email gateways can prevent some phishing attacks from reaching employees in the first place. Firewalls and antivirus software can mitigate the extent of any damage done by attackers who gain access to the network. Keeping operating systems updated with the latest patches can also close some vulnerabilities that attackers exploit through social engineering. Also, advanced detection and response solutions, including endpoint detection and response (EDR) and extended detection and response (XDR), can help security teams quickly detect and neutralize security threats that infect the network through social engineering tactics.

- dexebafadu
- http://fecirturizm.com/resimler/files/memoxa.pdf
- deruhi
- kuhifu
- how to cook rice in a crock pot
- amazing grace facts
- https://gesenerji.com/resimler/files/walefufubi.pdf
- cerebral angiogram vs dsa
- tafifa
- https://daithanhnam.com/upload/files/fikegolupanosen-mibikawulosewuj-ganojitumenabiw.pdf
- error sans canon height
- how to link traxxas tq 2.4
- masuvujuxi
- bixobikare
- gesekaca
- pigivu