Click Here

Social engineering in cybersecurity is the practice of manipulating someone into giving up sensitive information, usually through exploiting human error or taking advantage of trust in digital communications. How social engineering works Social engineering works by building false trust, exploiting human error, and using persuasion to gain access to sensitive or confidential information. As with most cyber threats, social engineering schemes can come in many forms, but they all generally work the same way. There are four basic steps to a successful social engineering attack: Preparation The social engineer gathers information about their victims, including where to contact them, such as on social media, email, text messaging platforms, etc. Infiltration The social engineer contacts their victims, often by impersonating a trustworthy source and using the information gathered about their victims to gain trust. Exploitation The social engineer uses persuasion to request information from their victims, such as contact information or even login details that they can use for fraudulent purposes. Disengagement After carrying out their attack, the social engineer abruptly breaks off communication with their victims. Depending on the social engineering attack type, these steps could span a matter of hours to months. But no matter the time frame, knowing the signs of a social engineering attack can help you stop it. An example of a social engineering attack happening through a text message. How to spot a social engineering attack If you receive a message from a stranger that feels random, too personal, or too good to be true it's likely the beginning of a social engineering attack. Unlike traditional cyberattacks where cybercriminals like to remain unnoticed, social engineers often communicate directly with their victims in plain sight. Here are some common social engineering techniques to watch out for: Strange messages Social engineers can pose as trusted individuals, including a friend, coworker, or even a bank. But you know your friends best, so if someone sends something out of the ordinary, ask them about it. Just use a different form of communication in case they were spoofed. Emotional manipulation Social engineers are great at stirring up specific emotions like fear, curiosity, or pity, so consider the cause of these emotional triggers before acting on them. If a complete stranger messages you with a sob story, it's likely a social engineering technique. Urgent requests Social engineers don't want you to think twice. That's why many social engineering attacks involve some type of urgency, such as a sweepstakes you need to enter immediately or cybersecurity software you need to download to wipe a supposed virus off your computer. Offers that feel too good to be true It's tempting to want to cash in on winning the lottery or go on a free cruise. But chances are that if the offer seems too good to be true, it is — it's probably a social engineering attack. Unsolicited help Social engineers might reach out pretending to be from a company providing help for a problem you don't have, like in a tech support scam. Don't be fooled into granting unsolicited remote access to your computer. False or unproven identity If you raise any suspicions with a potential social engineer and they're unable to prove their identity — perhaps they won't do a video call with you, for instance — chances are they're lying about who they are and what they want. 8 types of social engineering attacks + examples Almost all cyberattacks have some form of social engineering involved. And many social engineering techniques also involve malware — malicious software that wreaks havoc on devices and potentially monitors your activity. Here are some common forms of social engineering and examples, from in-person manipulation to annoying spam texts: 1. Scareware As the name indicates, scareware is malware that aims to scare you into doing something fast. It often comes in the form of pop-ups or emails imploring you to act immediately to get rid of supposed viruses or malware on your device. In fact, if you act you might be downloading a computer virus or malware. Scareware example — Imagine you're scrolling through your phone when you receive a message purporting to be from a popular messaging app telling you that the software version you're using is outdated and warning you against the dangers of not keeping your apps up to date. So, you click the provided link. But instead of the app being updated, your device is infected with malware. 2. Email hacking and contact spamming It's in our nature to pay attention to messages from people we know. And social engineers know this all too well, commandeering email accounts and spamming contact lists with all types of social engineering threats. Email hacking and contact spamming example — Your friend sends you an email with the subject, "Check out this site!" and you don't think twice before opening it. By hacking an email account, a social engineer can make contacts believe they're receiving emails from someone they know. Usually, the purpose is to spread malware or trick people into exposing their personal data. 3. Phishing Phishing is one of the most common types of social engineering, and typically involves a cybercriminal sending an email or text message asking for private information or encouraging you to click on an infected link. Different types of phishing scams are commonly used together, or in tandem with other social engineering schemes, to create more sophisticated social engineering attacks. Phishing scams also come in a few different delivery forms: Email phishing is one of the most traditional phishing methods and is often spam sent to many people at once. Vishing (voice phishing) is when a phisher calls or leaves a voicemail pretending to be from a trusted institution in hopes of gaining private information. Smishing (SMS phishing) involves sending texts containing malicious links or probing for personal information. URL phishing is when a phisher sends a link to a fake website that looks legitimate to the victim. When the victim clicks the link, they're asked to provide private details that can be harvested by the attacker. In-session phishing occurs when a victim is actively signed into an account or platform and a fake pop-up appears asking them to sign in again or to provide other sensitive information. It usually occurs on sites that don't use https encryption. Phishing example — Imagine you work for a big company, and you receive an email that appears to be from IT. The email asks you to change your login password immediately, but when you click the link provided, you're redirected to a fake site that collects your new login information. 4. DNS spoofing Also known as cache poisoning, DNS spoofing is when a browser is manipulated so that website visitors are redirected to malicious websites bent on stealing sensitive information. DNS spoofing is when your cache is poisoned with these malicious redirects. DNS spoofing example — A cybercriminal creates a convincing copycat site of an online marketplace. When users go to log in, they are rerouted to the fake site and enter their login details. By doing so, they've unwittingly shared their password and username with the cybercriminal. 5. Baiting Baiting is a social engineering technique that involves dangling something desirable in front of a victim, and hoping they'll take the bait — like rare access to a confidential file. This occurs most often on peer-to-peer sites like social media, whereby someone might encourage you to download a video or music, but it's actually malware. Baiting example — A social engineer leaves a USB stick that's loaded with malware in a public place. The USB is likely labeled in a compelling way — like "confidential" or "bonuses." A target picks up the device and plugs it into a computer to see what's on it, which loads the malware onto the device. 6. Pretexting Pretexting is the use of an interesting pretext, or ploy, to capture someone's attention. Once the story hooks the person, the social engineer tries to trick the would-be victim into providing something of value. Oftentimes, the social engineer is impersonating a legitimate source. Pretexting example — Let's say you receive an email naming you as the beneficiary of a will. The email requests your personal information to prove you're the actual beneficiary and to speed up the transfer of your inheritance. Instead, you're at risk of giving a con artist the ability to access and withdraw your funds. 7. Watering hole attacks A watering hole attack is a social engineering attack that infects a single website with malware. The site is almost always a very popular one — a virtual watering hole, if you will — to ensure that the malware can reach as many victims as possible. Watering hole attack example — In 2017, the Polish Financial Supervision Authority was the victim of a watering hole attack. In this social engineering attack, users from specific IP regions who visited the site were redirected to a custom exploit kit, which then installed malware onto the visitors' devices. 8. Quid pro quo Quid pro quo means a favor for a favor, essentially "I give you this, and you give me that." In this type of social engineering attack, the victim coughs up sensitive information, like account logins or financial details, then the social engineer doesn't return their end of the bargain. Quid pro quo example — Imagine you're on a gaming forum and on the lookout for a cheat code to pass a difficult level. You wire money to someone selling the code, but you never hear from them again and you don't get your code — you've fallen victim to a quid pro quo social engineering attack How to protect against social engineering attacks: 15 tips Avoid suspicious links and attachments. Don't click links or open attachments that you aren't expecting — they could be infected with malware or lead you to malicious websites. Don't overshare online. Social engineers know just what to look for when researching their victims. Protecting your privacy online is the first step to avoiding social engineering attacks. Use caution in online-only friendships. If an online friend is asking you for favors and personal information, but they're unwilling to verify their identity — be cautious. It might be a social engineer. Learn how to spot social engineering methods. Remember the signs of social engineering and the different ways social engineering attacks can affect you. Be skeptical. If a promise, offer, or deal seems too good to be true, it probably is. Grandiose promises are a common method of social engineering. Use two-factor authentication (2FA). Enabling 2FA on your online accounts can help keep your online data private and out of the hands of social engineers. Practice good password hygiene. Create strong, unique passwords and change them periodically. Never use the same password twice, and don't use common phrases or personal information. Use a password manager. Consider using a secure password manager to create hard-to-crack passwords and keep track of them all in one place. Set strict spam filters. Enable email and text spam filters to catch potential phishing messages. Social engineers love using spam messages to trick many victims at once. Keep your Wi-Fi network private. Don't allow strangers to access your Wi-Fi network — you don't know what they could be up to and what information they're collecting. Connect to a VPN. Use a VPN (virtual private network) when connecting to Wi-Fi, because encrypted data is private data, and can potentially save you from social engineering attacks. Monitor your account activity closely. If you notice unusual charges on your accounts, weird emails sent from your address, or other strange activity, change your passwords immediately. Don't leave devices unattended. Apart from avoiding theft, keeping track of your device helps you protect private data stored on your devices, such as account logins. And it also helps prevent physical breaches, like having a keylogger installed without your knowledge. Keep your software up to date. Using the best and most secure software on the market doesn't mean much unless you keep it up to date to avoid security vulnerabilities that hackers love to exploit. Use cybersecurity software. When social engineering attacks happen, cybersecurity software can help protect you from falling victim to cyberattacks. Manipulation is a nasty tactic for someone to get what they want. Thankfully, social engineering attacks can be thwarted if you know how to spot the signs. But knowledge isn't the only way to protect yourself against social engineering attacks. Norton 360 Deluxe is an all-in-one cybersecurity solution that can help protect your devices, your data, and yourself from falling victim. Editorial note: Our articles provide educational information for you. Our offerings may not cover or protect against every type of crime, fraud, or threat we write about. Our goal is to increase awareness about Cyber Safety. Please review complete Terms during enrollment or setup. Remember that no one can prevent all identity theft or cybercrime, and that LifeLock does not monitor all transactions at all businesses. The Norton and LifeLock brands are part of Gen Digital Inc. 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. Slides for Presentation on Real-World Social Engineering Attacks Lenny Zeltser , the free encyclopedia that anyone can edit. 110,331 active editors 7,023,424 articles in English Game Boy, platform of Donkey Kong Land Donkey Kong Land is a platform game developed by Rare and published by Nintendo for the Game Boy (pictured). Released on June 26, 1995, it condenses the side-scrolling gameplay of Donkey Kong Country with a different level design and boss fights. The player controls Donkey Kong and Diddy Kong as they recover their stolen banana hoard from King K. Rool. Development began in 1994: Rare's Game Boy programmer, Paul Machacek, developed Land as an original game rather than a port of Country, believing that it would be a better use of resources. Land features pre-rendered graphics converted to sprites through a compression technique. Rare retooled Country's gameplay to account for the lower-quality display, and David Wise and Graeme Norgate converted the soundtrack to the Game Boy's sound chip. Critics praised it as successfully translating Country's gameplay, visuals, and music to the Game Boy. Land was rereleased for the Nintendo 3DS and the Nintendo Switch. (Full article...) Recently featured: History of education in Wales (1701–1870) White dwarf Battle of Groix Archive By email More featured articles About Mendel Catholic High School ... that Mendel Catholic High School (pictured) raised $15 million through hosting weekly house dances from 1975? ... that singer Karin Ann made headlines after performing live on Polish state television wrapped in a rainbow flag? ... that voters approved a 600-percent increase in property taxes to fund programs at Valley Medical Center? ... that the Diocese of Poreč and Pula was nearly bankrupted over a dispute with the Italian Benedictines, a case that Dražen Kutleša is credited with quietly resolving? ... that the Dutch government considered converting the incomplete Java-class cruisers into English Channel ferries? ... that Jack Reardon received a heart transplant while serving as the mayor of Kansas City? ... that the symbol for equality in mathematics was not used for 61 years after its introduction, and was later popularized by Isaac Newton? ... that stand-up comedian Dustin Nickerson has said that his children have veto power over any jokes he might tell about them? ... that Saint-Saëns's Phaéton was described by a critic after its premiere as "the noise of a hack coming down from Montmartre"? Archive Start a new article Nominate an article Trifid and Lagoon nebulae The Vera C. Rubin Observatory in Chile releases the first light images (example shown) from its new 8.4-meter (28 ft) telescope. In basketball, the Oklahoma City Thunder defeat the Indiana Pacers to win the NBA Finals. An attack on a Greek Orthodox church in Damascus, Syria, kills at least 25 people. The United States conducts military strikes on three nuclear facilities in Iran. In rugby union, the Crusaders defeat the Chiefs to win the Super Rugby Pacific final. Ongoing: Gaza war Iran–Israel war Russian invasion of Ukraine timeline Sudanese civil war timeline Recent deaths: Maria Voce Wes Hildreth Lucien Nedzi Anne Burrell Frederick W. Smith Ron Taylor Nominate an article June 26 Douglas Skymaster plane Amana 1740 – War of Jenkins' Ear: Spanish troops stormed the British-held strategically crucial position of Fort Mose in Spanish Florida. 1945 – At a conference in San Francisco, delegates from 50 nations signed a charter establishing the United Nations. 1950 – A Douglas DC-4 Skymaster aircraft (pictured) crashed after departing from Perth, becoming the worst peacetime aviation accident in Australia's history. 2010 – A G20 summit, the largest and most expensive security operation in Canadian history, began in downtown Toronto. 2015 – The U.S. Supreme Court ruled in Obergefell v. Hodges that the right of same-sex couples to marry is guaranteed by the Fourteenth Amendment. Robert the Lotharingian (d. 1095)George IV of the United Kingdom (d. 1830)Walter C. Root (d. 1925)Pavel Belyayev (b. 1925) More anniversaries: June 25 June 26 June 27 Archive By email List of days of the year About Atacamite is a copper halide mineral: a copper(II) chloride hydroxide with the chemical formula Cu2Cl(OH)3. It was first described in 1802 by Dmitri Alekseyevich Golitsyn from deposits in Chile's Atacama Desert, after which it is named. Atacamite is a comparatively rare mineral, formed from primary copper minerals in the oxidation or weathering zone of arid climates. It has also been reported as a volcanic sublimate from fumarole deposits, as sulfide alteration products in black smokers. This photograph shows a specimen of atacamite, on a malachite matrix, from the Mount Gunson Mines in South Australia. The picture was focus-stacked from 42 separate images. Photograph credit: Ivar Leidus Recently featured: Turban Head eagle Springbok Geraldine Ulmar Archive More featured pictures Community portal – The central hub for editors, with resources, links, tasks, and announcements. Village pump – Forum for discussions about Wikipedia itself, including policies and technical issues. Site news – Sources of news about Wikipedia and the broader Wikimedia movement. Teahouse – Ask basic questions about using or editing Wikipedia. Help desk – Ask questions about using or editing Wikipedia. Reference desk – Ask research questions about encyclopedic topics. Content portals – A unique way to navigate the encyclopedia. Wikipedia is written by volunteer editors and hosted by the Wikimedia Foundation, a non-profit organization that also hosts a range of other volunteer projects: CommonsFree media repository MediaWikiWiki software development Meta-WikiWikimedia project coordination WikibooksFree textbooks and manuals WikidataFree knowledge base WikinewsFree-content news WikiquoteCollection of quotations WikisourceFree-content library WikispeciesDirectory of species WikiversityFree learning tools WikivoyageFree travel guide WiktionaryDictionary and thesaurus This Wikipedia is written in English. Many other Wikipedias are available; some of the largest are listed below. 1,000,000+ articles العربية Deutsch Español فارسی Français Italiano Nederlands 日本語 Polski Português Русский Svenska Українська Tiếng Việt 中文 250,000+ articles Bahasa Indonesia Bahasa Melayu Bân-lâm-gú Български Català Čeština Dansk Eesti Ελληνικά Esperanto Euskara עברית Հայերեն Magyar Norsk bokmål Română Simple English Slovenčina Srpski Srpskohrvatski Suomi Türkçe Oʻzbekcha 50,000+ articles Asturianu Azərbaycanca □□□□□ Bosanski کوردی Frysk Gaeilge Galego Hrvatski ქართული Kurdî Latviešu Lietuvių □□□□□□ Македонски □□□□□□□□□□□ Norsk nynorsk □□□□□□ Shqip Slovenš □□□ □□□□□□ اردو Retrieved from " 2 Calendar year Years Millennium 2nd millennium Centuries 17th century 18th century 19th century Decades 1720s 1730s 1740s 1750s 1760s Years 1737 1738 1739 1740 1741 1742 1743 vte October 9: The Batavia Massacre by the Dutch East India Company of at least 5,000 Chinese Indonesians begins in what is now Jakarta. 1740 by topic Arts and science Archaeology Architecture Art Literature Poetry Music Science Countries Canada Denmark France Great Britain Ireland Japan Norway Russia Scotland Spain Sweden Lists of leaders State leaders Colonial governors Religious leaders Birth and death categories Births Deaths Establishments and disestablishments categories Establishments Disestablishments Works category Works vte 1740 in various calendarsGregorian calendar1740MDCCXLAb urbe condita2493Armenian calendar1189ԹՎ ՌՃՁԹAssyrian calendar6490Balinese saka calendar1661–1662Bengali calendar1146–1147Berber calendar2690British Regnal year13 Geo. 2 – 14 Geo. 2Buddhist calendar2284Burmese calendar1102Byzantine calendar7248–7249Chinese calendar己未年 (Earth Goat)4437 or 4230 — to —庚申年 (Metal Monkey)4438 or 4231Coptic calendar1456–1457Discordian calendar2906Ethiopian calendar1732–1733Hebrew calendar5500–5501Hindu calendars - Vikram Samvat1796–1797 - Shaka Samvat1661–1662 - Kali Yuga4840–4841Holocene calendar11740Igbo calendar740–741Iranian calendar1118–1119Islamic calendar1152–1153Japanese calendarGenbun 5(元文５年)Javanese calendar1664–1665Julian calendarGregorian minus 11 daysKorean calendar4073Minguo calendar172 before ROC民前172年Nanakshahi calendar272Thai solar calendar2282–2283Tibetan calendar阴土羊年(female Earth-Goat)1866 or 1485 or 713 — to —阳金猴年(male Iron-Monkey)1867 or 1486 or 714 Wikimedia Commons has media related to 1740. 1740 (MDCCXL) was a leap year starting on Friday of the Gregorian calendar and a leap year starting on Tuesday of the Julian calendar, the 1740th year of the Common Era (CE) and Anno Domini (AD) designations, the 740th year of the 2nd millennium, the 40th year of the 18th century, and the 1st year of the 1740s decade. As of the start of 1740, the Gregorian calendar was 11 days ahead of the Julian calendar, which remained in localized use until 1923. Calendar year January 8 – All 237 crewmen on the Dutch East India Company ship Rooswijk are drowned when the vessel strikes the shoals of Goodwin Sands, off of the coast of England, as it is beginning its second voyage to the Indies. The wreckage is discovered more than 250 years later, in 2004.[1] February 20 – The North Carolina General Assembly incorporates the town of Newton as Wilmington, North Carolina, named for Spencer Compton, 1st Earl of Wilmington and patron of Royal Governor Gabriel Johnston. March 16 – King Edward of the Miskito Indians signs a treaty making his kingdom, located on the coast of modern-day Nicaragua, a protectorate of Great Britain.[2] March 25 – Construction begins on Bethesda Orphanage for boys near Savannah, Georgia, founded by George Whitefield. April 8 – War of the Austrian Succession: The Royal Navy captures the Spanish ship of the line Princesa off Cape Finisterre and takes her into British service. May 31 – Frederick II becomes King in Prussia upon the death of his father, Frederick William I. June 1 – Plantation Act 1740 or Naturalization Act 1740 of the Parliament of Great Britain comes into effect providing for Protestant alien immigrants (including Huguenots, and also Jews) residing in the American colonies for 7 years to receive British nationality. June 16 – Pour le Mérite first awarded in Prussia as a military honour. June 26 – War of Jenkins' Ear: Siege of Fort Mose – A Spanish column of 300 regular troops, free Black militia and Indian auxiliaries storms Britain's strategically crucial position of Fort Mose, Florida. July 7 – Adam Smith sets out from Scotland to take up a scholarship at Balliol College, Oxford.[3] July 11 – Pogrom: Jews are expelled from Little Russia. August 1 – The song Rule, Britannia! is first performed at Cliveden, the country home of Frederick, Prince of Wales, in England.[4] August 17 – Pope Benedict XIV succeeds Pope Clement XII, as the 247th pope. September 8 – Hertford College, Oxford, England, is founded for the first time.[5] October 9–22 – Batavia Massacre: Troops of the Dutch East India Company massacre 5,000–10,000 Chinese Indonesians in Batavia.[6] October 20 – Maria Theresa inherits the hereditary dominions of the Habsburg monarchy (Austria, Bohemia, Hungary and modern-day Belgium) under the terms of the Pragmatic Sanction of 1713 on the death of her father, Charles VI. Her succession to the Holy Roman Empire is contested widely because she is a woman, but she will reign for 40 years. November 6 – Samuel Richardson's popular and influential epistolary novel, Pamela; or, Virtue Rewarded, is published anonymously in London. November 14 – The University of Pennsylvania is officially established. December 16 – Frederick II of Prussia invades the Habsburg possession of Silesia, starting the War of the Austrian Succession. Enfield, North Carolina, is founded. Spain begins construction on Fort Matanzas in the Matanzas Inlet, approximately 15 miles (24 km) south of St. Augustine, Florida. The fairy-tale Beauty and the Beast by French novelist Gabrielle-Suzanne Barbot de Villeneuve was published. February 4 – Carl Michael Bellman, Swedish poet, composer (d. 1795) February 15 – Juan Andrés, Spanish Jesuit (d. 1817) February 16 – Giambattista Bodoni, Italian publisher and engraver (d. 1813) February 17 – John Sullivan, American General in the American Revolutionary War, delegate in the Continental Congress (d. 1795) March – Johann van Beethoven, German musician, father of Ludwig van Beethoven (d. 1792) March 16 – Johann Jacob Schweppe, German-born inventor, founder of the Schweppes Company (d. 1821) April 7 – Haym Salomon, Polish-Jewish American financier of the American Revolution (d. 1785) April 14 – Anna Strong, Patriot spy during the American Revolutionary War (d. 1812) May 7 – Nikolai Arkharov, Russian police chief (d. 1814) Marquis de Sade June 2 – Marquis de Sade, French author, for whom sadism is named (d. 1814) June 24 – Juan Ignacio Molina, Spanish-Chilean Jesuit priest, naturalist, historian, translator, geographer, botanist, ornithologist and linguist (d. 1829) June 27 – James Woodforde, English clergyman and diarist (d. 1803) July 27 – Jeanne Baré, French explorer (d. 1803) August 23 – Emperor Ivan VI of Russia (d. 1764) August 26 – Joseph-Michel Montgolfier, French inventor (d. 1810) September 12 – Johann Heinrich Jung, German writer (d. 1817) September 23 – Empress Go-Sakuramachi of Japan (d. 1813) September 25 – Hercules Mulligan, tailor and spy during the American Revolutionary War (d. 1825) October 29 – James Boswell, Scottish author (d. 1795) October 31 – Philip James de Loutherbourg, English artist (d. 1812) December – Elisabeth Olin, Swedish opera singer (d. 1828) Ali Pasha of Ioannina, Albanian ruler (d. 1822) Margaret Bingham, Countess of Lucan, born Margaret Smith, English portrait miniature painter and writer (d. 1814)[7] John Milton, American politician and officer of the Continental Army (d. 1817) (earliest estimated date of birth) Septimanie d'Egmont, French salonist (d. 1773) Pope Clement XII Frederick William I, King in Prussia Saint Theophilus of Corte Charles VI, Holy Roman Emperor Anna, Empress of Russia January – Louise Élisabeth de Joybert, politically active Canadian governors' wife (b. 1673) January 5 – Antonio Lotti, Italian composer (b. 1667) January 17 – Matthias Buchinger, German artist (b. 1674) January 20 – Niccolò Comneno Papadopoli, Italian jurist of religious law and historian (b. 1655) January 21 – Nicholas Trott, colonial magistrate, South Carolina Chief Justice (b. 1663) January 27 – Louis Henri, Duke of Bourbon, Prime Minister of France (b. 1692) January 29 – Richard Lumley, 2nd Earl of Scarbrough (b. 1686) February 6 – Pope Clement XII (b. 1652)[8] February 23 – Massimiliano Soldani Benzi, Italian artist (b. 1656) February 29 – Pietro Ottoboni, Italian cardinal (b. 1667) March 23 – Olof Rudbeck the Younger, Swedish scientist and explorer (b. 1660) April 28 – Bajirao I, Great Maratha warrior and Prime Minister of Marartha Empire (b.1700) April 23 – Thomas Tickell, English writer (b. 1685) May 17 – Jean Cavalier, French Protestant rebel leader (b. 1681) May 31 – Frederick William I, King in Prussia (b. 1688) June 1 – Samuel Werenfels, Swiss theologian (b. 1657) June 6 – Alexander Spotswood, British governor of Virginia Colony (b. 1676) June 17 Theophilus of Corte, Italian Roman Catholic priest, preacher and missionary, canonized (b. 1676) William Wyndham, English politician (b. 1687) June 18 – Piers Butler, 3rd Viscount Galmoye, Anglo-Irish nobleman (b. 1652) July 2 – Thomas Baker, English antiquarian (b. 1656) October 5 – Johann Philipp Baratier, German scholar (b. 1721) October 11 – Princess Magdalena Augusta of Anhalt-Zerbst, Duchess of Saxe-Gotha-Altenburg (b. 1679) October 20 – Charles VI, Holy Roman Emperor (b. 1685) October 28 – Anna, Empress of Russia (b. 1693) December 1 – John Abernethy, Irish Protestant minister (b. 1680) December 20 – Richard Boyle, 2nd Viscount Shannon, British military officer and statesman (b. 1675) December 30 – John Senex, English geographer (b. ca. 1678)[9] ^ Wendy van Duivenvoorde, Dutch East India Company Shipbuilding: The Archaeological Study of Batavia and Other Seventeenth-Century VOC Ships (Texas A&M University Press, 2015) p145 ^ "Mosquito Coast", in Historical Dictionary of the British Empire, ed. by Kenneth J. Panton (Rowman & Littlefield, 2015) p384 ^ "On this day in 1740..." Adam Smith Institute. July 7, 2010. Retrieved November 19, 2019. ^ Williams, Hywel (2005). Cassell's Chronology of World History. London: Weidenfeld & Nicolson. p. 308. ISBN 0-304-35730-8. ^ Hamilton, Sidney Graves (1903). Hertford College. University of Oxford college histories. London: Robinson. ^ "Image: Bird's eye view of Batavia showing the massacre of the Chinese". Archived from the original on September 21, 2009. Retrieved November 12, 2006. ^ This article incorporates text from a publication now in the public domain: Stephen, Leslie, ed. (1886). "Bingham, Margaret". Dictionary of National Biography. Vol. 5. London: Smith, Elder & Co. ^ "Clement XII | pope". Encyclopedia Britannica. Retrieved April 22, 2021. ^ "The Historical Theater in the Year 400 AD, in Which Both Romans and Barbarians Resided Side by Side in the Eastern Part of the Roman Empire". World Digital Library. 1725. Retrieved July 27, 2013. Retrieved from " 3One hundred years, from 1601 to 1700 Millennia 2nd millennium Centuries 16th century 17th century 18th century Timelines 16th century 17th century 18th century State leaders 16th century 17th century 18th century Decades 1600s 1610s 1620s 1630s 1640s 1650s 1660s 1670s 1680s 1690s Categories: Births – Deaths Establishments – Disestablishments vte The 17th century lasted from January 1, 1601 (represented by the Roman numerals MDCI), to December 31, 1700 (MDCC). It falls into the early modern period of Europe and in that continent (whose impact on the world was increasing) was characterized by the Baroque cultural movement, the latter part of the Spanish Golden Age, the Dutch Golden Age,[1] the French Grand Siècle dominated by Louis XIV, the Scientific Revolution, the world's first public company and megacorporation known as the Dutch East India Company, and according to some historians, the General Crisis. From the mid-17th century, European politics were increasingly dominated by the Kingdom of France of Louis XIV, where royal power was solidified domestically in the civil war of the Fronde. The semi-feudal territorial French nobility was weakened and subjugated to the power of an absolute monarchy through the reinvention of the Palace of Versailles from a hunting lodge to a gilded prison, in which a greatly expanded royal court could be more easily kept under surveillance. With domestic peace assured, Louis XIV caused the borders of France to be expanded. It was during this century that the English monarch became increasingly involved in conflicts with the Parliament - this would culminate in the English civil war and an end to the dominance of the English monarchy.A scene on the ice, Dutch Republic, first half of the 17th centuryBy the end of the century, Europeans were masters of logarithms, electricity, the telescope and microscope, calculus, universal gravitation, Newton's Laws of Motion, air pressure, and calculating machines due to the work of the first scientists of the Scientific Revolution, including Galileo Galilei, Johannes Kepler, René Descartes, Pierre Fermat, Blaise Pascal, Robert Boyle, Christiaan Huygens, Antonie van Leeuwenhoek, Robert Hooke, Isaac Newton, and Gottfried Wilhelm Leibniz. It was also a period of development of culture in general (especially theater, music, visual arts and philosophy). Some of the greatest inventions took place in this century. It was during this period that the European colonization of the Americas began in earnest, including the exploitation of the silver deposits, which resulted in bouts of inflation as wealth was drawn into Europe.[2] Also during this period, there would be a more intense European presence in Southeast Asia and East Asia (such as the colonization of Taiwan). These foreign elements would contribute to a revolution in Ayutthaya. The Mataram Sultanate and the Aceh Sultanate would be the major powers of the region, especially during the first half of the century.[2] In the Islamic world, the gunpowder empires – the Ottoman, Safavid, and Mughal – grew in strength as well. The southern half of India would see the decline of the Deccan Sultanates and extinction of the Vijayanagara Empire. The Dutch would colonize Ceylon and endure hostilities with Kandy. The end of the 17th century saw the first major surrender of Ottoman territory in Europe when the Treaty of Karlowitz ceded most of Hungary to the Habsburgs in 1699. In Japan, Tokugawa Ieyasu established the Tokugawa shogunate at the beginning of the century, beginning the Edo period; the isolationist Sakoku policy began in the 1630s and lasted until the 19th century. In China, the collapsing Ming dynasty was challenged by a series of conquests led by the Manchu warlord Nurhaci, which were consolidated by his son Hong Taiji and finally consummated by his grandson, the Shunzhi Emperor, founder of the Qing dynasty.[3] Qing China spent decades of this century with economic problems (results of civil wars between the Qing and former Ming dynasty loyalists), only recovering well at the end of the century. The greatest military conflicts of the century were the Thirty Years' War,[4] Dutch–Portuguese War,[5] the Great Turkish War, the Nine Years' War, Mughal-Safavid Wars, and the Qing annexation of the Ming. For a chronological guide, see Timeline of the 17th century. Main articles: 1600s, 1610s, 1620s, 1630s, and 1640s Persian Ambassador during his entry into Kraków for the wedding ceremonies of King Sigismund III of Poland in 1605. 1601: 4th Spanish Armada; in the Battle of Kinsale, England defeats Irish and Spanish forces, driving the Gaelic aristocracy out of Ireland and destroying the Gaelic clan system. 1601–1603: The Russian famine of 1601–1603 kills perhaps one-third of Russia.[6] 1602: Matteo Ricci produces the Map of the Myriad Countries of the World (坤輿萬國全圖, Kūnyú Wànguó Quántú), a world map that will be used throughout East Asia for centuries. 1602: The Dutch East India Company (VOC) is established by merging competing Dutch trading companies.[7] Its success contributes to the Dutch Golden Age. 1603: Elizabeth I of England dies and is succeeded by her cousin King James VI of Scotland, uniting the crowns of Scotland and England. 1603: Tokugawa Ieyasu takes the title of shōgun, establishing the Tokugawa shogunate. This begins the Edo period, which will last until 1868. 1603: In Nagasaki, the Portuguese Jesuit missionary João Rodrigues publishes Nippo Jisho, the first dictionary of Japanese to a European (Portuguese) language. 1605: The King of Gowa, a Makassarese kingdom in South Sulawesi, converts to Islam.Tsar Michael I of Russia reigned 1613–1645 1605–1627: The reign of Mughal emperor Jahangir after the death of emperor Akbar. 1606: The Long Turkish War between the Ottoman Empire and Austria is ended with the Peace of Zsitvatorok—Austria abandons Transylvania. 1606: Treaty of Vienna ends an anti-Habsburg uprising in Royal Hungary. 1606: Willem Janszoon captained the first recorded European landing on the Australian continent, sailing from Bantam, Java, in the Duyfken. 1607: Flight of the Earls (the fleeing of most of the native Gaelic aristocracy) occurs from County Donegal in the west of Ulster in Ireland. 1607: Iskandar Muda becomes the Sultan of Aceh for 30 years. He will launch a series of naval conquests that will transform Aceh into a great power in the western Malay Archipelago. 1610: The Polish–Lithuanian Commonwealth army defeats combined Russian–Swedish forces at the Battle of Klushino and conquers Moscow. 1610: King Henry IV of France is assassinated by François Ravaillac. 1611: The Pontifical and Royal University of Santo Tomas, the oldest existing university in Asia, is established by the Dominican Order in Manila[8] 1611: The first publication of the King James Bible. 1612: The first Cotswold Olympic Games, an annual public celebration of games and sports begins in the Cotswolds, England. 1613: The Time of Troubles in Russia ends with the establishment of the House of Romanov, which rules until 1917. 1613–1617: Polish–Lithuanian Commonwealth is invaded by the Tatars dozens of times.[9]James I of England and VI of Scotland ruled in the first quarter of the 17th century 1613: The Dutch East India Company is forced to evacuate Gresik due to the Mataram siege in neighboring Surabaya. The dutch negotiates with Mataram and is allowed to set up a trading post in Jepara. 1614–1615: The Siege of Osaka (last major threat to Tokugawa shogunate) ends. 1616: The last remaining Moriscos (Moors who had nominally converted to Christianity) in Spain are expelled. 1616: English poet and playwright William Shakespeare dies. 1618: The Defenestration of Prague. 1618: The Bohemian Revolt precipitates the Thirty Years' War, which devastates Europe in the years 1618–48. 1618: The Manchus start invading China. Their conquest eventually topples the Ming dynasty. 1619: European slaving reaches America when the first Africans are brought to the present-day United States. 1619: The Dutch East India Company storm Jayakarta and withstand a months-long siege by the combined English, Bantenese and Jayakartan forces. They are relieved by Jan Pieterszoon Coen and a fleet of ships from Ambon. The dutch destroys Jayakarta and builds its new headquarters, Batavia, on top of it. 1620–1621: Polish–Ottoman War over Moldavia. 1620: Bethlen Gabor allies with the Ottomans and an invasion of Moldavia takes place. The Polish suffer a disaster at Cecora on the River Prut. 1620: The Mayflower sets sail from Plymouth, England to what became the Plymouth Colony in New England.The 1622 massacre was instrumental in causing English colonists to view all natives as enemies 1621: The Battle of Chocim: Poles and Cossacks under Jan Karol Chodkiewicz defeat the Ottomans. 1622: Jamestown massacre: Algonquian natives kill 347 English settlers outside Jamestown, Virginia (approximately one-third of the colony's population)[10][11] and burn the Henricus settlement. 1624–1642: As chief minister, Cardinal Richelieu centralises power in France. 1626: St. Peter's Basilica in the Vatican completed. 1627: Aurochs go extinct.[12] 1628–1629: Sultan Agung of Mataram launches a failed campaign to conquer Dutch Batavia. 1629: Abbas I, the Safavids king, died. 1629: Cardinal Richelieu allies with Swedish Protestant forces in the Thirty Years' War to counter Ferdinand II's expansion. 1630: Birth of Shivaji at Shivneri fort, in present day Maharashtra, India, who later founded Maratha Empire in year 1674.[13] 1631: Mount Vesuvius erupts. 1632: Battle of Lützen, death of king of Sweden Gustav II Adolf.Battle of Nördlingen (1634). The Catholic Imperial army, bolstered by professional Habsburg Spanish troops won a great victory in the battle over the combined Protestant armies of Sweden and their German allies 1632: Taj Mahal building work started in Agra, India. 1633: Galileo Galilei arrives in Rome for his trial before the Inquisition. 1633–1639: Japan transforms into "locked country". 1634: Battle of Nördlingen results in Catholic victory. 1636: Harvard University is founded in Cambridge, Massachusetts. 1637: Shimabara Rebellion of Japanese Christians, rōnin and peasants against Edo. 1637: The first opera house, Teatro San Cassiano, opens in Venice. 1637: Qing dynasty attacked the Joseon dynasty. 1639: Naval Battle of the Downs – Republic of the United Provinces fleet decisively defeats a Spanish fleet in English waters. 1639: Disagreements between the Farnese and Barberini Pope Urban VIII escalate into the Wars of Castro and last until 1649. 1639–1651: Wars of the Three Kingdoms, civil wars throughout Scotland, Ireland, and England. 1640–1668: The Portuguese Restoration War led to the end of the Iberian Union.The inauguration of the Royal Academy of Turku in 1640. 1641: The Irish Rebellion, by Irish Catholics who wanted an end to discrimination, greater self-governance, and reverse ownership of the plantations of Ireland. 1641: René Descartes publishes Meditationes de prima philosophia Meditations on First Philosophy. 1642: Beginning of English Civil War, conflict will end in 1649 with the execution of King Charles I, the abolition of the monarchy and the establishment of the supremacy of Parliament over the king. 1643: L'incoronazione di Poppea, Monterverdi 1644: The Manchu conquer China ending the Ming dynasty. The subsequent Qing dynasty rules until 1912. 1644–1674: The Mauritanian Thirty-Year War. 1645–1669: Ottoman war with Venice. The Ottomans invade Crete and capture Canea. 1647–1652: The Great Plague of Seville. 1648: The Peace of Westphalia ends the Thirty Years' War and the Eighty Years' War and marks the ends of Spain and the Holy Roman Empire as major European powers.Map of Europe in 1648 at the end of the Thirty Years' War 1648–1653: Fronde civil war in France. 1648–1657: The Khmelnytsky Uprising – a Cossack rebellion in Ukraine which turned into a Ukrainian war of liberation from Poland. 1648–1667: The Deluge wars leave Polish–Lithuanian Commonwealth in ruins. 1648–1669: The Ottomans capture Crete from the Venetians after the Siege of Candia. 1649: King Charles I is executed for high treason, the first and only English king to be subjected to legal proceedings in a High Court of Justice and put to death. 1649–1653: The Cromwellian conquest of Ireland. Main articles: 1650s, 1660s, 1670s, 1680s, 1690s, and 1700s The Night Watch or The Militia Company of Captain Frans Banning Cocq, 1642. Oil on canvas; on display at the Rijksmuseum, Amsterdam 1651: English Civil War ends with the Parliamentarian victory at the Battle of Worcester. 1656–1661: Mehmed Köprülü is Grand Vizier. 1655–1661: The Northern Wars cement Sweden's rise as a Great Power. 1657 : Sambhaji, the second King of Maratha Empire and eldest son of King Shivaji was born at Purandar Fort on 14 May.[citation needed] 1658: After his father Shah Jahan completes the Taj Mahal, his son Aurangzeb deposes him as ruler of the Mughal Empire. 1659: King Shivaji killed Adil Shahi dynasty's general Afzal Khan at Pratapgad fort on 9 November.[14] 1660: The Commonwealth of England ends and the monarchy is brought back during the English Restoration. 1660: The Royal Society is founded. 1660: The Bruneian Civil War begins 1661: The reign of the Kangxi Emperor of China begins. 1663: Ottoman war against Habsburg Hungary. 1664: The Battle of St. Gotthard: count Raimondo Montecuccoli defeats the Ottomans. The Peace of Vasvar – intended to keep the peace for 20 years. 1665: Maratha King Shivaji signed the Treaty of Purandar with Mughal general Jai Singh I after Battle of Purandar.[citation needed] 1665: Robert Hooke discovers cells using a microscope. 1665: Portugal defeats the Kongo Empire at the Battle of Mbwila.Taj Mahal, completed by 1653 and commissioned by Shah Jahan, one of the Wonders of the World 1665–1667: The Second Anglo-Dutch War fought between England and the United Provinces. 1666: The Great Fire of London. 1666: Shivaji visited Aurangzeb at Agra Fort and forced him into house arrest. Shivaji later escaped and returned to the Maratha kingdom.[citation needed] 1667: The Raid on the Medway during the Second Anglo-Dutch War. 1667–1668: The War of Devolution: France invades the Netherlands. The Peace of Aix-la-Chapelle (1668) brings this to a halt. 1667–1699: The Great Turkish War halts the Ottoman Empire's expansion into Europe. 1672–1673: Ottoman campaign to help the Ukrainian Cossacks. John Sobieski defeats the Ottomans at the second battle of Khotyn (1673). 1672–1674: The Third Anglo-Dutch War fought between England and the United Provinces 1672–1676: Polish–Ottoman War.French invasion of the Netherlands, which Louis XIV initiated in 1672, starting the Franco-Dutch War 1672–1678: Franco-Dutch War. 1673: The Bruneian Civil War ends with Muhiyiddin winning the war. 1674: Shivaji founded the Maratha Empire and crowned himself as first Chatrapati of the empire. 1676–1681: Russia and the Ottoman Empire commence the Russo-Turkish Wars. 1678: The Treaty of Nijmegen ends various interconnected wars among France, the Dutch Republic, Spain, Brandenburg, Sweden, Denmark, the Prince-Bishopric of Münster, and the Holy Roman Empire.Claiming Louisiana for France in 1682 1680: The Pueblo Revolt drives the Spanish out of New Mexico until 1692. 1680: Prince Sambhaji crowned himself as the second Chatrapati of Maratha Empire 20 July.[citation needed] 1682: French explorer Robert La Salle claims all the land east of the Mississippi River.[15] 1683: China conquers the Kingdom of Tungning and annexes Taiwan. 1683: The Ottoman Empire is defeated in the second Siege of Vienna. 1683–1699: The Great Turkish War leads to the conquest of most of Ottoman Hungary by the Habsburgs. 1687: Isaac Newton publishes Philosophiae Naturalis Principia Mathematica. 1688: The Siege of Derry, the first major event in the Williamite War in Ireland. 1688: Siamese revolution of 1688 ousted French influence and virtually severed all ties with the West until the 19th century. 1688–1689: The Glorious Revolution starts with the Dutch Republic invading England, England becomes a constitutional monarchy. 1688–1691: The War of the Two Kings in Ireland. 1688–1697: The Grand Alliance sought to stop French expansion during the Nine Years' War. 1689: The Battle of Killiecrankie is fought between Jacobite and Williamite forces in Highland Perthshire. 1689: The Karposh rebellion is crushed in present-day North Macedonia, Skopje is retaken by the Ottoman Turks. Karposh is killed, and the rebels are defeated.The Battle of Vienna (1683) marked the historic end of the expansion of the Ottoman Empire into Europe 1689: Bill of Rights gains royal consent. 1689: John Locke publishes Two Treatises of Government and A Letter Concerning Toleration. 1690: The Battle of the Boyne in Ireland. 1692: Port Royal in Jamaica is struck by an earthquake and a tsunami. Approximately 2,000 people die and 2,300 are injured. 1692–1694: Famine in France kills two million.[16] 1693: College of William & Mary is founded in Williamsburg, Virginia, by a royal charter. 1694: The Bank of England is established. 1695: The Mughal Empire nearly bans the East India Company in response to pirate Henry Every's capture of the trading ship Ganj-i-Sawai. 1696–1697: Famine in Finland wipes out almost one-third of the population.[17] 1697–1699: Grand Embassy of Peter the Great to Western Europe. 1699: Thomas Savery demonstrates his first steam engine to the Royal Society. Catholic general Albrecht von Wallenstein (1583–1634), supreme commander of the armies of the Imperial Army during the Thirty Years War Jan Pieterszoon Coen (1587–1629), the founder of Batavia, was an officer of the Dutch East India Company (VOC), holding two terms as its Governor-General of the Dutch East Indies René Descartes (1596–1650) with Queen Christina of Sweden (1626–1689) Cardinal Mazarin (1602–1661), who served as the chief minister to the kings of France Louis XIII and Louis XIV Mughal Emperor Aurangzeb (1618–1707), who ruled over almost the entire Indian subcontinent for a period of 49 years Chhatrapati Shivaji (1630–1680) founder of Maratha Empire is widely regarded as one of the greatest Hindu rulers Kangxi Emperor (1661–1722) one of the most influential emperors of the Qing dynasty Shōgun Tokugawa Ieyasu was the founder of Japan's final shogunate, which lasted well into the 19th century See also: Timeline of historic inventions § 17th century Major changes in philosophy and science take place, often characterized as the Scientific Revolution. Banknotes reintroduced in Europe. Ice cream. Tea and coffee become popular in Europe. Central Banking in France and modern Finance by Scottish economist John Law. Minarets, Jamé Mosque of Isfahan, Isfahan, Persia (Iran), are built. 1604: Supernova SN 1604 is observed in the Milky Way. 1605: Johannes Kepler starts investigating elliptical orbits of planets. 1605: Johann Carolus of Germany publishes the 'Relation', the first newspaper. 1608: Refracting telescopes first appear. Dutch spectacle-maker Hans Lippershey tries to obtain a patent on one, spreading word of the invention. 1610: The Orion Nebula is identified by Nicolas-Claude Fabri de Peiresc of France. 1610: Galileo Galilei and Simon Marius observe Jupiter's Galilean moons. 1611: King James Bible or 'Authorized Version' first published. 1612: The first flintlock musket likely created for Louis XIII of France by

gunsmith Marin Bourgeois. 1614: John Napier introduces the logarithm to simplify calculations. 1616: Niccolò Zucchi describes experiments with a bronze parabolic mirror trying to make a reflecting telescope. 1620: Cornelis Drebbel, funded by James I of England, builds the first 'submarine' made of wood and greased leather. 1623: The third English dictionary, English Dictionarie, is published by Henry Cockeram, listing difficult words with definitions. 1628: William Harvey publishes and elucidates his earlier discovery of the circulatory system. 1637: Dutch Bible published. 1637: Teatro San Cassiano, the first public opera house, opened in Venice. 1637: Pierre de Fermat formulates his so-called Last Theorem, unsolved until 1995. 1637: Although Chinese naval mines were earlier described in the 14th century Huolongjing, the Tian Gong Kai Wu book of Ming dynasty scholar Song Yingxing describes naval mines wrapped in a lacquer bag and ignited by an ambusher pulling a rip cord on the nearby shore that triggers a steel-wheel flint mechanism. 1642: Blaise Pascal invents the mechanical calculator called Pascal's calculator. 1642: Mezzotint engraving introduces grey tones to printed images. 1643: Evangelista Torricelli of Italy invents the mercury barometer. 1645: Giacomo Torelli of Venice, Italy invents the first rotating stage. 1651: Giovanni Riccioli renames the lunar maria. 1656: Christiaan Huygens describes the true shape of the rings of Saturn. 1657: Christiaan Huygens develops the first functional pendulum clock based on the learnings of Galileo Galilei. 1659: Christiaan Huygens first to observe surface details of Mars. 1662: Christopher Merret presents first paper on the production of sparkling wine. 1663: James Gregory publishes designs for a reflecting telescope. 1669: The first known operational reflecting telescope is built by Isaac Newton. 1676: Antonie van Leeuwenhoek discovers Bacteria. 1676: First measurement of the speed of light. 1679: Binary system developed by Gottfried Wilhelm Leibniz. 1684: Calculus independently developed by both Gottfried Wilhelm Leibniz and Sir Isaac Newton and used to formulate classical mechanics. ^ "Exchange History NL – 400 years: the story". Exchange History NL. Archived from the original on 6 October 2022. Retrieved 6 October 2022. ^ a b "The Seventeenth-Century Decline". The Library of Iberian resources online. Retrieved 13 August 2008. ^ "5 of the 10 Deadliest Wars Began in China". Business Insider. 6 October 2014. ^ "The Thirty-Years-War". Western New England College. Archived from the original on 1999-10-09. Retrieved 2008-05-24. ^ Ames, Glenn J. (2008). The Globe Encompassed: The Age of European Discovery, 1500–1700. pp. 102–103. ^ Turchin, Peter (2009). Secular Cycles. Princeton University Press. pp. 256–257. ISBN 9780691136967. ^ Ricklefs (1991), page 28 ^ History of UST UST.edu.ph. Retrieved December 21, 2008. ^ "The Tatar Khanate of Crimea". Archived from the original on 2016-03-23. Retrieved 2008-06-05. ^ Mark, Joshua J. "Indian Massacre of 1622". World History Encyclopedia. Retrieved 2022-09-13. ^ Campbell, B.C (2008). Disasters, accidents, and crises in American history: A reference guide to the nation's most catastrophic events. Infobase Publishing. pp. 11–12. ^ Rokosz, M. (1995). "History of the Aurochs (Bos taurus primigenius) in Poland" (PDF). Animal Genetics Resources Information. 16: 5–12. doi:10.1017/S1014233900004582. Archived from the original (PDF) on 14 January 2013. ^ Itihas □□□□□□ [History, class fourth] (in Marathi). Maharashtra, India: Pathyapustak nirmiti madal, Pune. 2019. ^ "London museum correct record on general disembowelment by Chhatrapati Shivaji". The Tribune. ^ "René-Robert Cavelier, sieur de La Salle". Britannica. 30 March 2021. Retrieved 21 March 2021. ^ Alan Macfarlane (1997). The savage wars of peace: England, Japan and the Malthusian trap. Wiley . p. 64. ISBN 0-631-18117-2 ^ Karen J. Cullen (2010). "Famine in Scotland: The 'Ill Years' of the 1690s". Edinburgh University Press. p. 20. ISBN 0-7486-3887-3 Detail of a 17th-century Tekke Turkmen carpet Chang, Chun-shu, and Shelley Hsueh-lun Chang. Crisis and Transformation in Seventeenth-Century China (1998). Langer, William. An Encyclopedia of World History (5th ed. 1973); highly detailed outline of events online free Reid, A. J. S. Trade and State Power in 16th & 17th Century Southeast Asia (1977). Spence, J. D. The Death of Woman Wang: Rural Life in China in the 17th Century (1978). Clark, George. The Seventeenth Century (2nd ed. 1945). Hampshire, Stuart. The Age of Reason the 17th Century Philosophers, Selected, with Introduction and Interpretive Commentary (1961). Hugon, Cécile (1997) [1911]. "Social Conditions in 17th-Century France (1649-1652)". In Halsall, Paul (ed.). Social France in the XVII Century. London: Methuen. pp. 171–172, 189. ISBN 9780548161944. Archived from the original on 23 August 2016. Retrieved 7 August 2021. Lewitter, Lucian Ryszard. "Poland, the Ukraine and Russia in the 17th Century." The Slavonic and East European Review (1948): 157–171. in JSTOR Ogg, David. Europe in the Seventeenth Century (6th ed. 1965). Rowbotham, Sheila. Hidden from history: Rediscovering women in history from the 17th century to the present (1976). Trevor-Roper, Hugh R. "The general crisis of the 17th century." Past & Present 16 (1959): 31–64. Wikimedia Commons has media related to 17th century. Vistorica: Timelines of 17th century events, science, culture and persons Retrieved from " 4 The following pages link to 17th century External tools (link count transclusion count sorted list) · See help page for transcluding these entries Showing 50 items. View (previous 50 | next 50) (20 | 50 | 100 | 250 | 500)Astrology (links | edit) Alessandro Scarlatti (links | edit) Aurochs (links | edit) Bagpipes (links | edit) Drink (links | edit) List of decades, centuries, and millennia (links | edit) Kaohsiung (links | edit) Suffolk (links | edit) Waltz (links | edit) 20th century (links | edit) 15th century (links | edit) 16th century (links | edit) 18th century (links | edit) 1624 (links | edit) 1626 (links | edit) 1642 (links | edit) 1661 (links | edit) 1756 (links | edit) 1791 (links | edit) 1608 (links | edit) 1743 (links | edit) 14th century (links | edit) 1788 (links | edit) 1st century (links | edit) 13th century (links | edit) 1787 (links | edit) 4th century (links | edit) 12th century (links | edit) 11th century (links | edit) 1564 (links | edit) 1648 (links | edit) 1572 (links | edit) 1623 (links | edit) 1662 (links | edit) 1640s (links | edit) 1770s (links | edit) 1780s (links | edit) 1789 (links | edit) 1782 (links | edit) 1707 (links | edit) 1700s (decade) (links | edit) 1597 (links | edit) 1690 (links | edit) 1764 (links | edit) 1760s (links | edit) 1742 (links | edit) 1735 (links | edit) 1730s (links | edit) 1740s (links | edit) 1790s (links | edit) View (previous 50 | next 50) (20 | 50 | 100 | 250 | 500) Retrieved from " WhatLinksHere/17th_century" Cybercriminals are always trying to take advantage of organizations and employees who are not staying alert and up to date with the latest types of attacks. Refresh yourself about the types of attacks to watch for and the red flags that may help you spot them. Social Engineering Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or the best interest of your organization. The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network. Digital Attacks—Phishing Phishing is the most common digital attack, which is when you receive an email that looks like it's coming from a legitimate source, telling you that there's a problem which requires you to click a link or take an action that is in an attacker's interest. Digital Attacks—Spear Phishing Spear phishing is a small, focused attack via email on a particular person or organization. In this attack, the criminals research a specific target using social media and other open sources of information. In-Person Attacks—Tailgating A hacker scouts a location like the outside smoking area at your organization and then joins your group as a smoker, participating in your group conversation. When your group returns to work, he follows you in just like any other employee and then finds a workstation he can hack. A hacker may follow an employee to the building's locked entrance and walk in behind the employee or ask to be let in, saying that he forgot his key or access card. USB Attacks Attackers leave a USB stick that says "Payroll" where it can be easily found, like in your office parking lot, or sends it by mail disguised as a customer or vendor. Phone Attacks Another name for phone-based social engineering is voice phishing or "vishing." Like phishing, vishing is when the hacker calls you and tries to con you into surrendering confidential information. Phone Attacks—Smishing "Smishing" stands for "SMS phishing" or phishing that occurs through text messaging. For example, they send a text message asking you to call a number or click on a link. Red Flags Please keep an eye out for these red flags to help prevent security breaches: Someone unknown hanging around the building, even in a uniform. Others looking over your shoulder. Always lock your workstation if left unattended. E-mails that have strange "From" or "Reply to" addresses. Also, look at the "To" line and see if the e-mail was sent to many people. E-mails that come at strange times of day, or with strange or shocking subject lines. E-mails that ask you to click links within or open an attachment especially with content that makes you uncomfortable such as a security breach warning. Hyperlinks that contain strange or spoofed addresses. Hover over the link and look at the URL it will redirect you to. The one thing all of these attacks have in common is that they require a user to take action. Be alert and cautious to avoid these attacks. Think before you click! Protect your business with enterprise-grade, AI-enhanced email security tailored for SMBs and MSPs. Proofpoint Essentials multi-layered solution deploys quickly to safeguard your data, ensure business continuity, and block advanced cyber threats. Strengthen Office 365 Defense - Our robust system blocks advanced cyber threats like phishing and BEC. Key Features: Advanced threat detection, BEC prevention, email continuity, archiving, intelligent data protection. Ideal For: Small to medium sized businesses seeking powerful, easy-to-use email security, and MSPs protecting their clients. Scareware typically generates false alarms to convince users to install malicious software. These attacks rely on fictitious threats, such as fake antivirus warnings, to create a sense of urgency and fear, prompting victims to act quickly and without proper caution. Scareware manipulates users into making security mistakes, resulting in malware infections, data breaches, and financial loss. Avoiding tempting offers and suspicious alerts helps prevent installing software from untrusted sources. When COVID-19 spread around the planet, people were filled with emotions like fear, uncertainty and hope — which are the top ingredients for an effective social engineering campaign. Cyber criminals took full advantage of these emotions when disseminating malicious email spam attacks (malspam) across the globe.Read about the individual email spam attacks here: Malspam in the Time of COVID-19 > Threat Actor poses as CrowdStrike in Phishing ScamCrowdStrike Intelligence identified a callback phishing campaign impersonating prominent cybersecurity companies, including CrowdStrike itself. The phishing email implied that the recipient's company had been breached and insisted the victim call the included phone number. The hackers were ultimately after the victims' sensitive information.Read about the phishing scam here: Callback Malware Campaigns Impersonate CrowdStrike and Other Cybersecurity Companies >Malvertising Scam posed as Flash updateShlayer malvertising campaigns used fake Flash updates and social engineering tactics to trick victims into manually installing macOS malware and compromising their systems. Slayer is a type of malware that can quickly and discreetly infect a victim's system.Read about the malvertising scam here: Shlayer Malvertising Campaigns Using Flash Update Disguise >Social Engineering Attack PreventionThe best way to prevent social engineering threats is to take both a human and technological approach to your defense strategy.Best Practices to Prevent Social Engineering AttacksSecurity awareness training is the best way to prevent being victimized. Make sure your company has a process in place to allow employees to engage IT security personnel if they have any reason to believe they might be the victims of a social engineering attack.As a part of security awareness programs, organizations should continue to remind their employees of the following these common practices:DON'T CLICK ON LINKS SENT BY PEOPLE YOU DON'T KNOW. Hover over them first; trust but verify!Avoid opening attachments within emails from senders you do not recognize.Be wary of emails or phone calls requesting account information or requesting that you verify your account.Do not provide your username, password, date of birth, social security number, financial data or other personal information in response to an email or robocall.Always independently verify any requested information originating from a legitimate source.Always verify the web address of legitimate websites and manually type them into your browser.Check for misspellings or improper domains within a link (for example, an address that should end in a .gov ends in .com instead).Before transferring money or information, verify by voice or video call.Be alert to counterfeit items, such as sanitizing products and personal protective equipment, or people selling products that claim to prevent, treat, diagnose or cure COVID-19.Software to Prevent Social Engineering AttacksBeyond the human element, every organization should employ a cybersecurity solution that leverages the following capabilities:Sensor Coverage. You can't stop what you don't see. Organizations should deploy capabilities that provide their defenders with full visibility across their environment, to avoid blind spots that can become a safe haven for adversaries.Technical Intelligence. Leverage technical intelligence, such as indicators of compromise (IOCs), and consume them into a security information and event manager (SIEM) for data enrichment purposes. This allows for added intelligence when conducting event correlation, potentially highlighting events on the network that may have otherwise gone undetected. Implementing high-fidelity IOCs across multiple security technologies increases much-needed situational awareness.Threat Intelligence. Consuming narrative threat intelligence reports is a sure-fire method for painting a vivid picture of threat actor behavior, the tools they leverage and the tradecraft they employ. Threat intelligence assists with threat actor profiling, campaign tracking and malware family tracking. These days, it is more important to understand the context of an attack rather than just knowing an attack itself happened, and this is where threat intelligence plays a vital role.Threat Hunting. Understanding technology will only get organizations so far is more important now than ever before. Security technologies cannot guarantee 100% protection on their own, and understanding technology is not infallible is the first step in coming to grips with the need for 24/7, managed, human-based threat hunting. 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. 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. Social engineering is a staple term used in the email security world. Stories around John Podesta and his emails, Operation Wire Wire and great Defcon videos all have the expression "Social Engineering" stamped all over them. It's a key term in cyber security, and in an industry overrun with buzzwords, social engineering stands out in meaning, importance and scope. Social engineering techniques continue to wreak havoc on unsuspecting victims, and it's a trend that needs to be addressed. What is Social Engineering? "Social engineering" applies to the intentional and manufactured manipulation of people for the purposes of committing fraud. This fraud can be purely digital, or a combination of online and offline actions taken to deceive or compromise an individual or group. In the cyber security context, we focus on fraud that involves manipulating the relationship between digital technology and human behavior. This can be done on a targeted basis or through a "spray and pray" approach. The ends vary as well, ranging from planting trojans or backdoor exploits to committing invoice fraud to simply stealing a password. This form of manipulation uses tactics that have little difference from a high pressure sales scenario or aggressive marketing techniques, but in these cases are turned towards explicitly fraudulent or malicious ends. These tactics could include social proof, urgency/scarcity, reciprocity, authority, familiarity, consistency, and any combination thereof. What Isn't Social Engineering? That's a tricky question. In practice, likely the vast majority cyber security today involves some form of social engineering. Most of today's attacks involve a "social engineer" coming up with a campaign to gain access to a target and their data. A non-socially engineered attack would mean no human or social manipulation was involved. Examples that would not involve social engineering could include hacking, downloading code on non-secure websites (Drive-by Downloads), Bluetooth attacks, and plenty of others. But for many of the biggest attacks you hear about, they will almost without fail involve the intentional manipulation of a victim by a criminal through social engineering tactics, either with the victim making an error in judgement, or with some kind of deception that mixes in non-social engineering elements to achieve its goal. Breaking down the techniques used in Social Engineering Attacks Social engineering techniques make use of multiple strategies to get the end user to fall for their attacks. They will often overlap to improve the likelihood of success. Some of the techniques are more precise and targeted, focussing on the victim. Others will focus on conversion optimization – hoping to get any response to "pre-qualify the victim", and then work from there to extract funds from the victim. Here are a few of the most common social engineering techniques used: Mass Phishing The broadest and most generic of the social engineering techniques, mass or bulk phishing covers a very wide range of socially engineered threats towards 3 ends. Automated Money Extraction: Includes attacks such as Ransomware, often with the criminal having to only engineer the first click to be successful. Cyber Assisted Fraud: Requires engineering of the first action, followed by a grooming campaign to enable the fraud. Gaining Access to Data: This can be anything from credential phishing (victim filling out form on a malicious website) to installing exploits for large scale data extraction. The social engineering elements in a phishing attack range across the whole gamut of tactics. From creating urgency with (often faked) blackmail, social proof through sending emails out through a hacked email account, authority by spoofing a recognized brand, consistency by winding a long and persistent tale in a Nigerian Prince or Romance Scam and so on. Targeted Phishing An increasingly common means of social engineered attacks, targeted phishing can yield very high returns for con-artists. Generally, targeted phishing will involve a criminal researching a target at great lengths to be able to find details to exploit. The primary difference between bulk and targeted phishing is how personalized the content of the email campaign is. There are two areas of targeted phishing we see a lot of lately: Cyber-Assisted Fraud This term applies to a fraud that starts as a phishing attack to gain trust, access, or data, and then continues to an offline fraud. A common form of this is Business Email Compromise or CEO Fraud, where executives are impersonated or targeted to transfer money believing that the Invoice Fraud These (targeted or not) can trick a recipient into believing there's an outstanding invoice, and immediate payment is required. A tactic commonly used in these attacks is gaining access to a potential victim's email address. The criminal can forward all emails to his own account waiting until an important deal or transaction is supposed to go through. At that point, he or she will send across an email with instructions to modify payment details (for examples) or even call to limit the trail. This happens often in real estate or legal industries where large transactions are common. Baiting (mostly Trojan) This is possibly the oldest form of social engineering (if the Iliad is our guide). It is named after the technique of hiding something in plain site so that an unsuspecting victim welcomes a hidden virus in. A criminal can target messaging to the recipient to maximize the possibility of getting the download or link click. Under this, we would include Quid Pro Quo – where the target is offered something for free, say an eCard or game download in exchange for a piece of confidential information (often a password or even a contact list). Malicious Email Attachment Attacks Similar to baiting, the attachment you download that you think is a presentation or holiday pictures, can download viruses, malware, and trojans to all kinds of malicious ends. Again, these are often engineered to optimize the probability of conversion and to minimize the resistance that the end user might put up. Vishing Vishing, or voice phishing, involves the use of the telephone to gain access to confidential information, usually credit cards or passwords. This form of social engineering plays off a trust we have in our phones and in voices that we don't have for emails. Similar tactics or used in Smishing or SMS Phishing. A common example of this would be an automated call aiming to get you to enter your credit card or password details, from a company that you possibly have an account in. Social Media Attacks While they are a form of phishing attacks, they deserve a special mention because of their unique methodology in engineering the social proof elements. For those who are vulnerable, getting an unsolicited friend request from a (usually) good looking member of the opposite gender can lead down a rocky path. This is especially true when the con-artist is using a well groomed persona with a strong accompanying cover (read:sob) story. An evolution of the 419ers or Romance scams, these are more effective then their predecessors as they include more of the elements of a social engineered attack. Fake news/Market Manipulation/Political Sabotage Increasing with the spread of fake news, the manipulation of people's perceptions illegally through various technological means big payoffs, political or financial. Examples of this include spam campaigns for stock market manipulation ("Pump and dump") which could spread a lie rapidly while the criminal holds a position. Fake crowdsourcing campaigns, fake news stories, fake Video and much more will will lead to all kinds of engineered attacks. Social Engineering Isn't Going Anywhere With the increasing impact of everything integrated, always on, and connected, the stakes are high. At the same time cyber security is advancing rapidly requiring criminals to be constantly seeking out new ways to earn a "living". The most reliable and time proven method of successful fraud has been social engineering and conning people out of their money. Of the socially engineering threats that involve technology, many can be mitigated. Anti-virus and malware protection, email security, attachment protection, URL defense are a few examples. Machine learning, AI and even blockchain technology, will make it harder for human error to be as costly. However, for the inattentive employee, CEO or political campaign manager, there will always be fraud. —- Have a laugh at this comedian's work while you are at it. Online only. W/ new line on myPlan. No trade-in required. With select Verizon Home internet plans. With new line on myPlan. No trade-in required. W/ select phone trade-in & myPlan req'd. Service plan req'd for watch and tablet. Online only. Limited time offer. With new line on Unlimited Ultimate. w/ Unlimited Welcome & Auto Pay. Plus taxes & fees. W/ 4 new smartphones. Experience nation-wide mobile coverage with plans for every budget. Enjoy reliable home internet with no annual contracts. Bundle your mobile & home internet for exclusive benefits. 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? Enjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch NowEnjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch NowEnjoy sharper detail, more accurate color, lifelike lighting, believable backgrounds, and more with our new model update. Your generated images will be more polished than ever.See What's NewExplore how consumers want to see climate stories told today, and what that means for your visuals.Download Our Latest VisualGPS ReportData-backed trends. Generative AI demos. Answers to your usage rights questions. Our original video podcast covers it all—now on demand.Watch Now Cybersecurity research summary. Cybersecurity threats pose a greater risk than ever before. More and more people rely on modern technology, and an increasing number of U.S. and international businesses use digital devices and web-based software. After extensive research, our data analysis team found the following cybersecurity facts and data breach statistics: Cyberattacks happen once every 39 seconds. 95% of cyberattacks are due to human error. Cybercrime cost people in the United States an estimated $6.9 billion in 2021. Globally, an estimated 30,000 websites are hacked each day. 43% of Cyberattacks target small businesses. Only 5% of company folders and files are properly protected. Cybersecurity was likely a concern for you whether you know how many people get hacked a year or not. Regardless, knowing the facts can really drive home just how big of an issue cybersecurity has become in the modern world. Here are some general statistics around cybersecurity you should know: Cybercrime costs the global economy $6 trillion each year. The cost of cybercrime is increasing significantly and is expected to grow by as much as 15% over the next five years. It's estimated that by 2025, cybercrime will cost the world roughly $10.5 trillion every year. Almost all cybersecurity breaches are due to human error. It's estimated that a whopping 95% of all cybersecurity breaches are a result of human error. Cybercriminals often target small businesses, infiltrating their websites and distributing malicious code to web users who view or interact with the site. As such, although these security breaches are usually tied to human error, business owners and their customers are often unaware of any threat. Today, many experts view cybersecurity breaches as one of the biggest threats to mankind. Some of the best ways of avoiding a cyberattack include keeping your web server software up to date, encrypting web traffic when transferring personal information, performing routine virus scans, and frequently backing up your website. It's estimated that the United States spends about $3.5 billion annually on cybersecurity. In 2019, the United States spent a reported $3.5 billion combating cyberattacks, according to the Federal Bureau of Investigation. Although that number represents the yearly average spent by the U.S. on cybersecurity, the actual dollar amount is likely much higher as many attacks go unnoticed and unrecorded. In fact, one security firm estimated that ransomware alone costs the U.S. an estimated $9 billion yearly. In addition, the cost of cybersecurity is only increasing. In 2020, U.S. businesses spent about 23% more on cybersecurity than the previous year. However, the increasing dollar amount was still met with increasing digital security breaches. Meanwhile, across the world, cybersecurity is expected to cost $10.5 trillion by 2025. Across the world, the United States spends the most on cybersecurity. Averaging a $3.5 billion (or more) average annual cybersecurity budget, the U.S. tops every other country in the world when it comes to cybersecurity preparedness and spending. This year, in fact, the American government is expected to allocate an additional $18.78 billion investment in cybersecurity. Behind the United States, other top spenders include Israel, Iran, Canada, Malaysia, Australia, France, Spain, and the United Kingdom. The FBI's Internet Crime Complaint Center (IC3) reported 847,376 complaints in 2021. This is a 7% increase from 2020. Top complaints involved ransomware, business e-mail compromise (BEC) schemes, and the criminal use of cryptocurrency. The IC3 reported a $6.9 billion loss for the American public in 2021. This is up from $4.2 billion in 2020. This number has been steadily increasing since 2017, when it was at $1.4 billion. Year Reported Complaints Financial Loss 2021 847,376 $6.9 Billion 2020 791,790 $4.2 Billion 2019 467,361 $3.5 Billion 2018 351,937 $2.7 Billion 2017 301,580 $1.4 Billion Cybersecurity is an issue for corporations all over the world. Of the accounts that get hacked and data that gets breached, those at the corporate level are some of the least explored and most damaging incidents. Here are some crucial examples of the harm poor cybersecurity can do at the corporate level: More than half of all U.S. companies have experienced phishing. Roughly 62% of organizations in the United States have experienced social engineering and phishing attacks. In cybersecurity, phishing refers to the practice of attempting to gain access to sensitive information by sending a company or individual an online scam that appears to come from a reputable source. On average, 5% of a company's files are properly protected from cyber threats. At just 5%, only a very small amount of an average business' sensitive and private files are properly protected from hackers, according to the 2019 Varonis Global Data Risk Report. Moreover, data suggests that 22% of all folders in a given company are open to every employee, and as many as 53% of companies have more than 1,000 sensitive files open to every employee. 43% of cyberattacks target small businesses. While just shy of 50% of all cyberattacks targeting small businesses, only 14% of those organizations are prepared to defend themselves against digital attacks. In fact, six out of every ten small businesses have no cybersecurity protection in place. Although small businesses are a top target for data breaches, 66% of senior decision-makers at small businesses in the United States believe they are not at risk. Cyberattacks can some from many different sources, and under many different strategies. Here are some hacker statistics that dive into the methodology behind Cyberattacks: More than 40% of data breaches involved internal actors. Data suggests that 43% of data breaches involve internal actors, including employees, contractors, and third-party suppliers. It's estimated that half of all data breaches that involve internal actors are intentional, while the other half are accidental. During cyberattacks, internal actors are more likely to target employee information, including identification and health data, as opposed to customer data, according to Mcafee's Grand Theft Data report. Email is the most common method hackers use when delivering malware. In the first six months of 2021, roughly 75% of all cybersecurity threats were delivered via email, according to the HP Wolf Security Threat Insights Report. Data suggests that 49% of phishing emails are about business transactions, while 16% consist of generic names, numbers, and letters. Mobile devices account for 60% of cyber fraud. Phishing attacks on mobile devices are becoming more and more common, with cell phones now accounting for 60% of cyber fraud. Increased international reliance on cell phones, mobile banking, and the use of mobile devices for sensitive business have all contributed to the growing rate of mobile cyber fraud. Most malware attacks target Windows systems. Roughly 83.45% of malware was detected on Windows devices in the first quarter of 2020. Meanwhile, 11.09% is detected on browsers, and 3.24% is detected on Androids. Roughly 1.91% of malware is detected on other systems. Thousands of ransomware attacks occur each day. Since 2016, roughly 4,000 ransomware attacks have happened every day. In the United States, ransomware represents the fastest growing malware threat, according to the Federal Bureau of Investigation. The FBI's IC3 reports the top internet crime in 2021 was phishing. There were 323,972 reported phishing incidents in the U.S. in 2021. Additionally, non-payment/nondelivery, personal data breach, identity theft, and extortion make up the next four most common forms of cybercrime. Top 5 reported internet crimes in 2021 Internet Crime Reported Incidents Phishing 323,972 Non-Payment/Non-Delivery 82,478 Personal Data Breach 51,829 Identity Theft 51,629 Extortion 39,360 Hackers can target almost anyone, but there are certain targets more vulnerable to cybersecurity threats than others. Here are some common hacking target trends: Approximately 3.8 million records are exposed by hackers every day. From 2013 through today, it's estimated that 3,809,448 records have been and continue to be exposed by hackers every single day. At this rate, 158,727 documents are exposed every hour, 2,645 documents are exposed every minute, and as many as 44 records are exposed every second. Hackers primarily target government, retail, and technology industries. Roughly 95% of all cybersecurity breaches happen in government, retail, and technology markets. Experts suggest this high-risk rate is due to the fact that these markets have a large number of personal records and sensitive information, including credit card information, social security numbers, and computer passwords in their digital files. Outside of these three markets, the healthcare industry is also often targeted by digital hackers. In 2020 alone, 75% of healthcare facilities in the United States were infected with malicious software at some point during the year. Individuals have much lower chances of getting hacked. Approximately 111.7 million Americans are hacked each year. Records indicate that as many as one in three Americans have their data breached every year, totally roughly 111.7 million individuals. Most personal data breaches on U.S. citizens can be linked to insecure usernames and passwords and a lack of digital literacy. The average cost of a digital data breach in the U.S. is $200,000. For all companies, big and small, a cybersecurity attack costs, on average, $200,000. While more American companies have become proactive in their mission to ward off cyberattacks, the rate at which breaches happen continues to increase. Due to the debilitating costs associated with digital data breaches, an estimated 60% of American businesses are forced to shut their doors within six months of being attacked. The average ransom demand is more than $150,000. Today, the average ransom demand is $178,254 — 60% more than the early 2020 average of $111,605. It's estimated that more than one-third of all companies who are attacked with ransomware pay that price (or a similar one) within 16 days. Roughly 1 million new pieces of malware are made each day. Historical data suggests that more than 317 million computer viruses, or malware, are created every year. At that rate, nearly 1 million new viruses are created each day. Cybersecurity trends and projections are always changing along with technology an the new strategies deployed by hackers. Knowing that, we've gathered all of the latest cybersecurity trends: Cyberattacks rose 400% during the pandemic. During the height of the COVID-19 pandemic, cyberattacks were up as much as 400%, according to the Federal Bureau of Investigation. Prior to the pandemic, the FBI received approximately 1,000 daily complaints to its Internet Crime Complaint Center. COVID-19 closures and the transition to a remote work environment, meanwhile, caused those complaints to rise to 3,000 to 4,000 per day. Cybersecurity costs are projected to grow by 15% per year over the next five years. Globally, cybersecurity is expected to cost roughly $6 trillion this year. Over the next several years, that number is estimated to grow by at least 15% per year, totaling $10.5 trillion in 2025. There has been a recorded 151% increase in ransomware attacks in early 2021. In the second quarter of 2021, ransomware attacks totaled 304.7 million, with the FBI warning that there are 100 new strains circulating the world. Meanwhile, in 2020 a total of 304.6 million ransomware attacks were recorded for the entire year. How many Cyberattacks happened in 2020? 155.8 million digital U.S. records were exposed as a result of cyberattacks, and approximately 1,001 major data breaches were recorded in the United States in 2020. Meanwhile, globally an estimated 30,000 websites were hacked each day. In addition, every year since 2016 — 2020 included — have seen roughly 4,000 international ransomware attacks, representing a 300% increase since 2015. What does social engineering mean in cybersecurity? In cybersecurity, social engineering refers to the practice of manipulating vulnerable parties to forfeit private and sensitive information online. When hackers use social engineering, they aim to exploit human errors in order to access confidential data and spread malicious malware and computer viruses. How many accounts are hacked each day in the US? About half a million U.S. accounts are hacked every day. Since 2015, an average of 199.17 million digital records have been exposed each year in the United States Overall, it's estimated that about one in three Americans are hacked every year. Are cybersecurity threats increasing? Yes, cybersecurity threats are increasing. Early 2021 saw a 151% increase in ransomware attacks alone, reaching 304.7 million attacks. That's more attacks than there were in all of 2020, which saw 304.6 million ransomware attacks. Other cyberattacks increased during 2020 and 2021 as well. As a significant portion of the U.S. workforce shifted to remote work during the COVID-10 pandemic, cyberattacks increased by 400%, and the FBI went from receiving about 1,000 cyberattack complaints a day to up to 4,000. The number of cybersecurity threats is only expected to increase, as experts estimate that there are 1 million new pieces of malware (aka computer viruses) being created each day and that to combat these and other threats, cybersecurity costs will increase by 15% each year from 2020 to 2025. This means global cybersecurity costs will grow from $6 trillion in 2021 to $10.5 trillion in 2025 as governments and private businesses alike work to protect themselves from cyberattacks of all kinds. How many data breaches happened in 2021? 1,862 data breaches happened in 2021. This set a new record previously held by 2017 and its 1,506 data breaches. This 2021 figure was also a 68% increase from the 2020s 1,108 breaches. Experts believe that cybercriminals shifted their focus toward smaller, more precise attacks rather than trying to steal as much data as possible in 2021, which resulted in a 5% decrease in the number of people who were affected by these attacks. Still, 294 million people were impacted by data breaches. Ransomware attacks accounted for 22% of reported cyberattacks in 2021. This kind of attack has been growing rapidly over the past few years, putting it on pace to surpass phishing as the most common cause of data breaches. The military is the only sector that didn't report a single data breach during 2021, while manufacturing and utilities saw the number of breaches they experienced more than double from 2020 to 2021. CNet. "Data Breaches Break Record in 2021." Accessed on April 1, 2022. What is the most common data breach? Phishing is the most common data breach. In 2019, this form of cybercrime accounted for almost one-third of all Cyberattacks, and the number of phishing attacks increased during the COVID-19 pandemic. Phishing is when someone sends a malicious link via email, text, or social media that looks legitimate but is designed to steal information or install malicious software when opened. During the first half of 2021, about 75% of all cybersecurity attacks were made via email, the majority of which was likely some form of phishing. However, social media is becoming a more popular site for phishing schemes, as people are often more willing to trust the direct messages they receive on those platforms. 95% of all cyberattacks are due to human error, and more than half of U.S. companies have experienced phishing, which shows just how big of a threat this is. Ransomware attacks are becoming increasingly common, though, accounting for 22% of cyberattacks in 2021, and they're slated to continue to grow until they surpass phishing as the number one type of data breach. Safeguard Cyber. "Phishing Attacks Are What Percentage of Cyberattacks?" Accessed on April 1, 2022. Are data breaches increasing? Yes, data breaches are increasing. 2021 saw a 68% increase in the number of reported data breaches, which added up to 1,862 breaches. This even beat 2017's previous record of about 1,500 breaches. As people moved to more remote work during the COVID-19 pandemic, they began using more mobile devices, which are often more susceptible to data breaches. (Mobile phones account for 60% of cyber fraud.) As a result, the number of breaches was able to increase exponentially. While phishing is still widely considered the most common cyberattack method, the number of ransomware attacks is increasing rapidly. This type of cyberattack made up 22% of 2021's breaches and is continuing to grow, putting it on pace to take over phishing's spot as the most common type of cyberattack. 294 million people were affected by 2021's data breaches, so companies and governments are working hard to improve their cybersecurity so they can protect the information people have entrusted them with. As a result, though, it's expected that cybersecurity costs will increase by 15% year over year from 2021 to 2025. Cybersecurity breaches remain one of the biggest threats to economic and financial stability, business success, and the protection of personal property and information.While spending on cybersecurity protection increases, cyberattacks show no real sign of slowing down.The U.S. spends roughly $3.5 billion per year on cybercrime costs, a number which is only expected to increase this year after a record 400% increase in cyberattacks during the peak of the coronavirus pandemic. Also climbing are global costs, which are expected to reach as much as $10.5 trillion by 2025.With an international cyberattack happening once every 39 seconds, knowledge could be the nation's greatest digital protection, as an estimated 95% of attacks are directly linked to human error. Cobalt. "Business Cost Of Cybercrime." Accessed on November 14, 2021. Bank Info Security. "Ransomware Payday: Average Payments Jump To $178,000." Accessed on November 14, 2021. Cybercrime Magazine. "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Accessed on November 14, 2021. Forbes. "30,000 Websites Hacked A Day. How Do You Host Yours?" Accessed on November 14, 2021. University Of North Georgia. "Cybersecurity: A Global Priority And Career Opportunity." Accessed on November 14, 2021. Analytics India Magazine. "Top Cybersecurity Budgets Around The World." Accessed on November 15, 2021. Varonis. "2019 Varonis Global Data Risk Report." Accessed on November 15, 2021. CNBC. "Cyberattacks Now Cost Companies $200,000 On Average, Putting Many Out Of Business." Accessed on November 15, 2021. CNN Business. "Nearly 1 Million New Malware Threats Released Every Day." Accessed on November 15, 2021. Statista. "Cyber Crime: Number Of Breaches And Records Exposed 2005-2020." Accessed on November 15, 2021. Mcafee. "Grand Theft Data." Accessed on November 16, 2021. ZDNet. "HP Finds 75% Of Threats Were Delivered By Email In First Six Months Of 2021." Accessed on November 16, 2021. Reader's Digest. "Top Security Threats Of Smartphones (2021)." Accessed on November 16, 2021. Statista. "Distribution Of Malware Detections Q1 2020, By OS." Accessed on November 16, 2021. Federal Bureau Of Investigation. "How To Protect Your Networks From

Ransomeware." Accessed on November 16, 2021. Threat Post. "Ransomware Volumes Hit Record Highs As 2021 Wears On." Accessed on November 16, 2021. The Hill. "FBI Sees Spike In Cyber Crime Reports During Coronavirus Pandemic." Accessed on November 16, 2021. PR Newswire. "Top Cyber Security Experts Report: 4,000 Cyber Attacks A Day SInce COVID-19 Pandemic." Accessed on November 16, 2021. Federal Bureau of Investigation "Internet Crime Report 2021" Accessed on February 27, 2023. Social engineering is a manipulation technique that deceives individuals or groups to exploit or gain unauthorized access to sensitive information or resources. Since most humans like to help, this cyberattack targets human vulnerabilities rather than technical vulnerabilities by using psychological tactics to exploit our curiosity or impulse to trust.Falling victim to social engineering could lead to unauthorized access to personal, financial, or organizational data; identity theft; financial loss; or compromised network security. To combat social engineering, question suspicious or unsolicited emails, calls, or visits. Be skeptical before providing personal, sensitive, or proprietary data. Educate yourself about security awareness. If they're using an urgent or emotional appeal, think twice. Install strong security protocols such as two-factor or multi-factor authentication to make it more difficult for social engineers to get into your accounts with their illicitly gained information. What are some of the most common social engineering techniques?Almost every type of cybersecurity attack has some traits of social engineering, here are some common methods that attackers use:Phishing: Attackers send deceptive emails or messages designed to persuade you to click on a link, download a malicious file, or provide sensitive data.Smishing: Bad actors use messaging, such as texting or WhatsApp, to get you to send payments, download attachments, or provide personal information.Spoofing: Cybercriminals create websites that look like they belong to legitimate organizations to trick you into revealing sensitive information. Baiting: This involves leaving physical or digital devices, such as infected USB drives, in strategic locations to tempt individuals into using them. You're trying to help and get that device back to its rightful owner but you unknowingly grant access or compromise your systems.Pretexting: An attacker takes on an alternative persona to entice you to disclose data or your access credentials. Often they will appear to be authority figures, such as the IRS or a business supervisor.Tailgating: Someone gains unauthorized entry to a restricted area in a physical location, such as a building, by following closely behind a person who is allowed to enter. The individual might appear as a repair person, or they might come up with their hands full of balloons and a cake and ask you to hold the door open for them.Quid pro quo: This involves offering something of value, such as a gift or service, in exchange for personal information or access to systems. When you see something that's too good to be true—say free Apple products—don't fall for this type of social engineering. Someone offering your IT support in return for your access information is another common version of quid pro quo.Learn how to fight social engineering scams on Coursera Take the next step toward a career in cybersecurity by enrolling in the Google Cybersecurity Professional Certificate on Coursera. This Professional Certificate is your gateway to exploring job titles like security analyst SOC (security operations center) analyst, and more. Upon completion, you'll have exclusive access to a job platform with over 150 employees hiring for entry-level cybersecurity roles and other resources supporting your job search. 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. Stay ahead of threats with news and insights on security, AI and more, weekly in the Think Newsletter. 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. Related solutions IBM X-Force IBM X-Force's threat-centric team of hackers, responders, researchers and analysts help protect your organization from global threats. Explore IBM X-Force Threat detection and response solutions IBM threat detection and response solutions strengthen your security and accelerate threat detection. Explore threat detection solutions X-Force Red Penetration Testing Services IBM X-Force Red provides penetration testing services for applications, networks, hardware and personnel to uncover and fix vulnerabilities. Explore penetration testing services Social engineering is the act of exploiting human weaknesses to gain access to personal information and protected systems. Social engineering relies on manipulating individuals rather than hacking computer systems to penetrate a target's account. Social engineering is illegal.Social engineering attacks can happen to an individual online or in person.Identity theft is a social engineering attack.There are many precautions you can take from creating a two-step authentication system for your accounts to using a different password for each account.There are many forms of social engineering attacks, but the most common is phishing. Social engineering refers to the manipulation of a target so that they give up key information. In addition to stealing an individual's identity or compromising a credit card or bank account, social engineering can be applied to obtain a company's trade secrets or exploit national security. For example, a woman might call a male victim's bank, pretend to be his wife, claim an emergency, and request access to his account. If the woman can successfully socially engineer the bank's customer service representative by appealing to the representative's empathetic tendency, she may succeed in obtaining access to the man's account and stealing his money. Similarly, an attacker might contact an email provider's customer service department to obtain a password reset, making it possible for the attacker to control a target's email account rather than hacking into that account. Social engineering is complex for potential targets to prevent. Precautions such as strong passwords and two-factor authentication for accounts can be used, but accounts can still be compromised by third parties with access to accounts, such as bank employees. However, individuals can decrease their risk in many ways. These include avoiding giving out confidential information, being cautious when sharing information on social media, and not repeating passwords to your accounts. Additional ways to decrease hacking are using two-factor authentication, using fake or difficult-to-guess answers to account security questions, and keeping a close eye on accounts, particularly financial ones. Set your spam filters to high to keep out unwanted messages, and never open an attachment without careful consideration of what it contains. And it is always a wise decision to pay close attention to any emails that seem suspicious or out of the ordinary, even if they seem to come from someone or a business you know. Attackers often use surprisingly simple tactics in social engineering schemes, such as asking people for help. Another tactic is to exploit disaster victims by asking them to provide personally identifiable information such as maiden names, addresses, dates of birth, and social security numbers for missing or deceased loved ones. Why? Because these pieces of information can later be used for identity theft. Posing as a tech-support professional or a delivery person is easy to gain unauthorized access to an account, as is sending a seemingly legitimate email with a malicious attachment. Such emails are often sent to a work email address where people are less likely to be suspicious of an unknown sender. Emails can be disguised to appear as though they have originated from a known sender when they are sent by a hacker. More elaborate tactics targeted to specific people might involve learning about their interests and then sending the target a link related to that interest. The link can contain malicious code that can steal personal information from their computers. Popular social engineering techniques include phishing, catfishing, tailgating, and baiting. If you aren't expecting a link or attachment from a friend or colleague, it may even be worth a phone call or text to them to find out if they did send it to rule out a scammer. There are many ways hackers create social engineering attacks, from posing as a tech support professional offering to "fix" a bug in your computer to sending you a "friend" request to your social media account. Here are three popular social engineering attacks. Online baiting occurs when hackers send out ads with links that look like opportunities to find jobs, earn side money, or appear to provide useful information. When an unsuspecting person clicks on the bait, malware infects their computer. These scams are done in the form of texts or emails that impersonate a bank or other financial institution, or even a government office, claiming you have violated a policy, forgotten to pay your taxes, or asking you to change your password. These scams are designed to elicit fear or concern from the receiver and get them to give out sensitive information. These types of attacks lure unsuspecting individuals to provide personal information such as bank account numbers, social security numbers, and other sensitive information with the hacker's goal of breaching your financial accounts. Social engineering attacks don't just happen online. Physical interactions can occur, such as an individual pretending to work in your office, and asking you to let them in because they "forgot the door code or their card key," and need help. Phishing used to obtain social security numbers, addresses, and other forms of personal information is the most common form of social engineering. Social engineering is extremely common and hackers and scammers are becoming more sophisticated in their methods. Yes. Social engineering attacks are illegal, and some forms, such as identity theft or breaking into a government facility, are considered serious crimes. Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems. Attacks can happen online, in-person, and via other interactions. Scams based on social engineering are built around how people think and act. As such, social engineering attacks are especially useful for manipulating a user's behavior. Once an attacker understands what motivates a user's actions, they can deceive and manipulate the user effectively. In addition, hackers try to exploit a user's lack of knowledge. Thanks to the speed of technology, many consumers and employees aren't aware of certain threats like drive-by downloads. Users also may not realize the full value of personal data, like their phone number. As a result, many users are unsure how to best protect themselves and their information. Generally, social engineering attackers have one of two goals: Sabotage: Disrupting or corrupting data to cause harm or inconvenience. Theft: Obtaining valuables like information, access, or money. This social engineering definition can be further expanded by knowing exactly how it works. How Does Social Engineering Work? Most social engineering attacks rely on actual communication between attackers and victims. The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data. The attack cycle gives these criminals a reliable process for deceiving you. Steps for the social engineering attack cycle are usually as follows: Prepare by gathering background information on you or a larger group you are a part of. Infiltrate by establishing a relationship or initiating an interaction, started by building trust. Exploit the victim once trust and a weakness are established to advance the attack. Disengage once the user has taken the desired action. This process can take place in a single email or over months in a series of social media chats. It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware. It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts. By masquerading as legitimate users to IT support personnel, they grab your private details — like name, date of birth or address. From there, it's a simple matter to reset passwords and gain almost unlimited access. They can steal money, disperse social engineering malware, and more. Traits of Social Engineering Attacks Social engineering attacks center around the attacker's use of persuasion and confidence. When exposed to these tactics, you are more likely to take actions you otherwise wouldn't. Among most attacks, you'll find yourself being misled into the following behaviors: Heightened emotions : Emotional manipulation gives attackers the upper hand in an any interaction. You are far more likely to take irrational or risky actions when in an enhanced emotional state. The following emotions are all used in equal measure to convince you. Fear Excitement Curiosity Anger Guilt Sadness Urgency: Time-sensitive opportunities or requests are another reliable tool in an attacker's arsenal. You may be motivated to compromise yourself under the guise of a serious problem that needs immediate attention. Alternatively, you may be exposed to a prize or reward that may disappear if you do not act quickly. Either approach overrides your critical thinking ability. Trust: Believability is invaluable and essential to a social engineering attack. Since the attacker is ultimately lying to you, confidence plays an important role here. They've done enough research on you to craft a narrative that's easy to believe and unlikely to rouse suspicion. There are some exceptions to these traits. In some cases, attackers use more simplistic methods of social engineering to gain network or computer access. For example, a hacker might frequent the public food court of a large office building and "shoulder surf" users working on their tablets or laptops. Doing so can result in a large number of passwords and usernames, all without sending an email or writing a line of virus code. Now that you understand the underlying concept, you're probably wondering "what is social engineering attack and how can I spot it?" Types of Social Engineering Attacks Almost every type of cybersecurity attack contains some kind of social engineering. For example, the classic email and virus scams are laden with social overtones. Social engineering can impact you digitally through mobile attacks in addition to desktop devices. However, you can just as easily be faced with a threat in-person. These attacks can overlap and layer onto each other to create a scam. Here are some common methods used by social engineering attackers: Phishing Attacks Phishing attackers pretend to be a trusted institution or individual in an attempt to persuade you to expose personal data and other valuables. Attacks using phishing are targeted in one of two ways: Spam phishing, or mass phishing, is a widespread attack aimed at many users. These attacks are non-personalized and try to catch any unsuspecting person. Spear phishing and by extension, whaling , use personalized info to target particular users. Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials. Whether it's a direct communication or via a fake website form, anything you share goes directly into a scammer's pocket. You may even be fooled into a malware download containing the next stage of the phishing attack. Methods used in phishing each have unique modes of delivery, including but not limited to: Voice phishing (vishing) phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you to increase trust and urgency. SMS phishing (smishing) texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number. Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used. Angler phishing takes place on social media, where an attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack. Search engine phishing attempt to place links to fake websites at the top of search results. These may be paid ads or use legitimate optimization methods to manipulate search rankings. URL phishing links tempt you to travel to phishing websites. These links are commonly delivered in emails, texts, social media messages, and online ads. Attacks hide links in hyperlinked text or buttons, using link-shortening tools, or deceptively spelled URLs. In-session phishing appears as an interruption to your normal web browsing. For example, you may see such as fake login pop-ups for pages you're currently visiting. Baiting Attacks Baiting abuses your natural curiosity to coax you into exposing yourself to an attacker. Typically, potential for something free or exclusive is the manipulation used to exploit you. The attack usually involves infecting you with malware. Popular methods of baiting can include: USB drives left in public spaces, like libraries and parking lots. Email attachments including details on a free offer, or fraudulent free software. Physical Breach Attacks Physical breaches involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information. Attacks of this nature are most common in enterprise environments, such as governments, businesses, or other organizations. Attackers may pretend to be a representative of a known, trusted vendor for the company. Some attackers may even be recently fired employees with a vendetta against their former employer. They make their identity obscure but believable enough to avoid questions. This requires a bit of research on the attacker's part and involves high-risk. So, if someone is attempting this method, they've identified clear potential for a highly valuable reward if successful. Pretexting Attacks Pretexting uses a deceptive identity as the "pretext" for establishing trust, such as directly impersonating a vendor or a facility employee. This approach requires the attacker to interact with you more proactively. The exploit follows once they've convinced you they are legitimate. Access Tailgating Attacks Tailgating , or piggybacking, is the act of trailing an authorized staff member into a restricted-access area. Attackers may play on social courtesy to get you to hold the door for them or convince you that they are also authorized to be in the area. Pretexting can play a role here too. Quid Pro Quo Attacks Quid pro quo is a term roughly meaning "a favor for a favor," which in the context of phishing means an exchange of your personal info for some reward or other compensation. Giveaways or offers to take part in research studies might expose you to this type of attack. The exploit comes from getting you excited for something valuable that comes with a low investment on your end. However, the attacker simply takes your data with no reward for you. DNS Spoofing and Cache Poisoning Attacks DNS spoofing manipulates your browser and web servers to travel to malicious websites when you enter a legitimate URL. Once infected with this exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved. DNS cache poisoning attacks specifically infect your device with routing instructions for the legitimate URL or multiple URLs to connect to fraudulent websites. Scareware Attacks Scareware is a form of malware used to frighten you into taking an action. This deceptive malware uses alarming warnings that report fake malware infections or claim one of your accounts has been compromised. As a result, scareware pushes you to buy fraudulent cybersecurity software, or divulge private details like your account credentials. Watering Hole Attacks Watering hole attacks infect popular webpages with malware to impact many users at a time. It requires careful planning on the attacker's part to find weaknesses in specific sites. They look for existing vulnerabilities that are not known and patched — such weaknesses are deemed zero-day exploits . Other times, they may find that a site has not updated their infrastructure to patch out known issues. Website owners may choose delay software updates to keep software versions they know are stable. They'll switch once the newer version has a proven track record of system stability. Hackers abuse this behavior to target recently patched vulnerabilities. Unusual Social Engineering Methods In some cases, cybercriminals have used complex methods to complete their cyberattacks, including: Fax-based phishing: When one bank's customers received a fake email that claimed to be from the bank — asking the customer to confirm their access codes – the method of confirmation was not via the usual email / Internet routes. Instead, the customer was asked to print out the form in the email, then fill in their details and fax the form to the cybercriminal's telephone number. Traditional mail malware distribution: In Japan, cybercriminals used a home-delivery service to distribute CDs that were infected with Trojan spyware. The disks were delivered to the clients of a Japanese bank. The clients' addresses had previously been stolen from the bank's database. Examples of Social Engineering Attacks Malware attacks deserve a special focus, as they are common and have prolonged effects. When malware creators use social engineering techniques, they can lure an unwary user into launching an infected file or opening a link to an infected website. Many email worms and other types of malware use these methods. Without a comprehensive security software suite for your mobile and desktop devices, you're likely exposing yourself to an infection. Worm Attacks The cybercriminal will aim to attract the user's attention to the link or infected file – and then get the user to click on it. Examples of this type of attack include: The LoveLetter worm that overloaded many companies' email servers in 2000. Victims received an email that invited them to open the attached love letter. When they opened the attached file, the worm copied itself to all of the contacts in the victim's address book. This worm is still regarded as one of the most devastating, in terms of the financial damage that it inflicted. The Mydoom email worm — which appeared on the Internet in January 2004 — used texts that imitated technical messages issued by the mail server. The Swen worm passed itself off as a message that had been sent from Microsoft. It claimed that the attachment was a patch that would remove Windows vulnerabilities. It's hardly surprising that many people took the claim seriously and tried to install the bogus security patch — even though it was really a worm. Malware Link Delivery Channels Links to infected sites can be sent via email, ICQ and other IM systems — or even via IRC Internet chat rooms. Mobile viruses are often delivered by SMS message. Whichever delivery method is used, the message will usually contain eye-catching or intriguing words that encourage the unsuspecting user to click on the link. This method of penetrating a system can allow the malware to bypass the mail server's antivirus filters. Peer-to-Peer (P2P) Network Attacks P2P networks are also used to distribute malware. A worm or a Trojan virus will appear on the P2P network but will be named in a way that's likely to attract attention and get users to download and launch the file. For example: AIM & AOL Password Hacker.exe Microsoft CD Key Generator.exe PornStar3D.exe Play Station emulator crack.exe Shaming Infected Users out of Reporting an Attack In some cases, the malware creators and distributors take steps that reduce the likelihood of victims reporting an infection: Victims may respond to a fake offer of a free utility or a guide that promises illegal benefits like: Free Internet or mobile communications access. The chance to download a credit card number generator. A method to increase the victim's online account balance. In these cases, when the download turns out to be a Trojan virus, the victim will be keen to avoid disclosing their own illegal intentions. Hence, the victim will probably not report the infection to any law enforcement agencies. As an example of this technique, a Trojan virus was once sent to email addresses that were taken from a recruitment website. People that had registered on the site received fake job offers, but the offers included a Trojan virus. The attack mainly targeted corporate email addresses. The cybercriminals knew that the staff that received the Trojan would not want to tell their employers that they had been infected while they were looking for alternative employment. How to Spot Social Engineering Attacks Defending against social engineering requires you to practice self-awareness. Always slow down and think before doing anything or responding. Attackers expect you to take action before considering the risks, which means you should do the opposite. To help you, here are some questions to ask yourself if you suspect an attack: Are my emotions heightened? When you're especially curious, fearful, or excited, you're less likely to evaluate the consequences of your actions. In fact, you probably will not consider the legitimacy of the situation presented to you. Consider this a red flag if your emotional state is elevated. Did this message come from a legitimate sender? Inspect email addresses and social media profiles carefully when getting a suspect message. There may be characters that mimic others, such as "torn@example.com" instead of "tom@example.com." Fake social media profiles that duplicate your friend's picture and other details are also common. Did my friend actually send this message to me? It's always good to ask the sender if they were the true sender of the message in question. Whether it was a coworker or another person in your life, ask them in-person or via a phone call if possible. They may be hacked and not know, or someone may be impersonating their accounts. Does the website I'm on have odd details? Irregularities in the URL, poor image quality, old or incorrect company logos, and webpage typos can all be red flags of a fraudulent website. If you enter a spoofed website, be sure to leave immediately. Does this offer sound too good to be true? In the case of giveaways or other targeting methods, offers are a strong motivation to drive a social engineering attack forward. You should consider why someone is offering you something of value for little gain on their end. Be wary at all times because even basic data like your email address can be harvested and sold to unsavory advertisers. Attachments or links suspicious? If a link or file name appears vague or odd in a message, reconsider the authenticity of the whole communication. Also, consider if the message itself was sent in an odd context, time, or raises any other red flags. Can this person prove their identity? If you cannot get this person to verify their identity with the organization, they claim to be a part of, do not allow them the access they are asking for. This applies both in-person and online, as physical breaches require that you overlook the attacker's identity. How to Prevent Social Engineering Attacks Beyond spotting an attack, you can also be proactive about your privacy and security. Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users. Here are some important ways to protect against all types of cyberattacks: Safe Communication and Account Management Habits Online communication is where you're especially vulnerable. Social media, email, text messages are common targets, but you'll also want to account for in-person interactions as well. Never click on links in any emails or messages . You'll want to always manually type a URL into your address bar, regardless of the sender. However, take the extra step of investigating to find an official version of the URL in question. Never engage with any URL you have not verified as official or legitimate. Use multi-factor authentication. Online accounts are much safer when using more than just a password to protect them. Multi-factor authentication adds extra layers to verify your identity upon account login. These "factors" can include biometrics like fingerprint or facial recognition, or temporary passcodes sent via text message. Use strong passwords (and a password manager). Each of your passwords should be unique and complex. Aim to use diverse character types, including uppercase, numbers, and symbols. Also, you will probably want to opt for longer passwords when possible. To help you manage all your custom passwords, you might want to use a password manager to safely store and remember them. Avoid sharing names of your schools, pets, place of birth, or other personal details. You could be unknowingly exposing answers to your security questions or parts of your password. If you set up your security questions to be memorable but inaccurate, you'll make it harder for a criminal to crack your account. If your first car was a "Toyota," writing a lie like "clown car" instead could completely throw off any prying hackers. Be very cautious of building online-only friendships. While the internet can be a great way to connect with people worldwide, this is a common method for social engineering attacks. Watch for tells and red flags that indicate manipulation or a clear abuse of trust. Safe Network Use Habits Compromised online networks can be another point of vulnerability exploited for background research. To avoid having your data used against you, take protective measures for any network you're connected to. Never let strangers connect to your primary Wi-Fi network. At home or in the workplace, access to a guest Wi-Fi connection should be made available. This allows your main encrypted, password-secured connection to remain secure and interception-free. Should someone decide to "eavesdrop" for information, they won't be able to access the activity you and others would like to keep private. Use a VPN . In case someone on your main network — wired, wireless, or even cellular — finds a way to intercept traffic, a virtual private network (VPN) can keep them out. VPNs are services that give you a private, encrypted "tunnel" on any internet connection you use. Your connection is not only guarded from unwanted eyes, but your data is anonymized so it cannot be traced back to you via cookies or other means. Keep all network-connected devices and services secure. Many people are aware of internet security practices for mobile and traditional computer devices. However, securing your network itself, in addition to all your smart devices and cloud services is just as important. Be sure to protect commonly overlooked devices like car infotainment systems and home network routers. Data breaches on these devices could fuel personalization for a social engineering scam. Safe Device Use Habits Keeping your devices themselves is just as important as all your other digital behaviors. Protect your mobile phone, tablet, and other computer devices with the tips below: Use comprehensive internet security software. In the event that social tactics are successful, malware infections are a common outcome. To combat rootkits, Trojans and other bots, it's critical to employ a high-quality internet security solution that can both eliminate infections and help track their source. Don't ever leave your devices unsecured in public. Always lock your computer and mobile devices, especially at work. When using your devices in public spaces like airports and coffee shops, always keep them in your possession. Keep all your software updated as soon as available. Immediate updates give your software essential security fixes. When you skip or delay updates to your operating system or apps, you are leaving known security holes exposed for hackers to target. Since they know this is a behavior of many computer and mobile users, you become a prime target for socially engineered malware attacks. Check for known data breaches of your online accounts. Services like Kaspersky Antivirus Software 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: Social engineering is a form of psychological manipulation intended to trick users into making security mistakes or giving up sensitive information that can be used for fraudulent purposes. These "scammers'' use tactics such as fear, pressure, baiting and other forms of manipulation to exploit or fool their unsuspecting target(s) into handing over sensitive information. These "scammers," commonly known as "bad actors," are mainly motivated by financial gain. The impact of social engineering can hurt both the individual and larger organization. This finding is corroborated by the FBI's most recent Internet Crime Report, which found phishing, vishing, smishing, pharming the No. 1 cyber crime type by volume accounting for over 323,972 victims. The impact of social engineering attacks is growing as the corporate attack surface expands and cloud-based systems become more pervasive. According to the 2022 Verizon Data Breach Investigations Report (DBIR), a top industry recognized report created annually to help minimize risk and keep your business safe, social engineering is defined as the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality. The impact of social engineering is purely attributed to the "human element" with an enormous 82% of breaches accounted for by social attacks, human errors and misuse. Additionally, as the DBIR states, malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program. These attacks continue to be split between phishing attacks and the more convincing pretexting attacks, which are commonly associated with business email compromises (BEC). These are the two main types of integrity violations. Pretexting: The bad actor often pretends to be in a position of authority in order to trick the victim into getting what they need. Pretexting accounts for 27% of social engineering breaches, almost all of which are BECs. Phishing: The bad actor impersonates a legitimate user or institution via email and uses fear, urgency or curiosity to trick an employee into clicking malicious links, opening malware-laden attachments or handing over login credentials. 41% of BECs involved phishing. It's important to note this trickery is also prevalent via smishing (text message compromise) and vishing (via voice tactics). The negative consequences of successful social engineering can be significant: Stealing users' personal and financial data which can be sold or used fraudulently. Stealing corporate logins (with a view to deploy ransomware, steal data, access cloud email servers, etc.). Deploying malware through malicious links/attachments, with command and control (C2), backdoors and Trojans as the most common malware varieties. Tricking users into making money transfers or buying/sending gift cards. Social engineering attacks are constantly maturing in nature. For instance, Google's Threat Analysis Group (TAG), "[In 2021]...identified an ongoing campaign targeting security researchers working on vulnerability research and development at different companies and organizations. The actors behind this campaign, which we attribute to a government-backed entity based in North Korea, have employed a number of means to target researchers…" including the creation of a sophisticated Twitter campaign to appear legitimate. The impact of social engineering on the organization can put anyone at considerable risk. Here are some of the latest social engineering assault trends: These packages offer hackers with few technical skills all the resources they need to launch phishing campaigns, including databases of targets and phishing templates. One vendor detected a 397.5% increase in domains associated with phishing kits from September to November 2021. The FBI revealed new scams in which deepfake audio is used in conjunction with virtual meetings to trick employees into wiring funds on behalf of their "CEO." In reality, it's not their CEO but spoofed audio played on top of a still image. The scammers typically make an excuse about technical issues preventing the video from working properly. Multi-factor authentication (MFA) fatigue is when attackers use (often stolen) credentials to login and trigger repeated MFA requests in the hopes that the user will ultimately accept a request. Some more sophisticated attackers are going further and posing as IT to "help" resolve these MFA "issues". If the user then provides MFA directly to this fake IT request, the attacker can gain access to the system. We are now seeing highly-customized spear-phishing attacks - especially targeted at c-suite executives - that leverage personal information scraped from social media and even purchased on the dark web. Though not a new technique, phone-based phishing (vishing) has become a popular way to increase the impact of social engineering on the organization. IBM found click rates for phishing campaigns surged threefold when vishing was included. The Federal Communications Commission is now treating ID spoofing as a consumer protection priority. One tactic seeks to exploit a well-known document drive's notification system. By tagging their target in a comment on a document containing malicious links to a phishing site, and asking them to collaborate, the target receives a legitimate email notification containing the comment's text and a link to the relevant document. Instead of harvesting users' passwords, some social engineering attacks use OAuth permission request screens to trick users into granting access tokens. This enables the attacker to access victim accounts, steal confidential info, maintain persistence and perform other tasks. Microsoft warns such consent phishing attacks are on the rise. Like most cyber attacks, the impact of social engineering on the organization can ultimately be measured in significant financial and reputational damage, illustrated by the following statistics: Contributing factors to breach costs arising from social engineering include: IT overtime (investigation and response) Recovery and remediation Legal costs Lost productivity and sales Regulatory fines Customer churn Although a social engineering attack is difficult to fully prevent, you can take steps to mitigate the threat. Here are some best practices and recommendations: Company wide cyber security training: Training can help stop problems before they start. Look for a security provider that is able to provide actionable insights to help organizations of all sizes implement robust cybersecurity policies and solutions to better respond to threats. Enhanced end-user awareness training: Campaigns should be run regularly in short lessons of 10-15 minutes across the entire organization. Real-life simulations are key, as is the ability to analyze and act on the results. Zero trust: Leverage a zero trust architecture so as to limit access to tools and systems. Regular backups: According to the best practice 3-2-1 methodology, create three backups to two different types of media with one stored off-site. Process changes: Consider internal changes that would mandate checks before large money transfers are approved. Email security tools: Use email security tools to spot suspicious links, attachments, domains and behavior. Artificial intelligence-powered capabilities can also scan for writing-style changes that indicate phishing. Good cyber hygiene: Employ continuous risk-based patching to mitigate the impact of social engineering on the organization. Multi-factor authentication/password managers: This will help reduce the typical risk associated with corporate passwords. Incident response (IR): Create and regularly test IR plans to ensure the organization can recover quickly from a breach. Regular pen testing will also help reveal any exposure to social engineering. Threat detection tools: Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) can help to uncover malicious activity following a successful social engineering attack. Managed security services: For organizations short on internal skills and resources, third-party providers can help out with many of the above capabilities. The Verizon Threat Research Advisory Center can help your organization stay up to date on the latest trends in social engineering attacks. Learn more about how to secure your attack surface and secure your business. Gabriela Allen is the Head of Security Product Marketing at Verizon Business Group.