Unit-5

Social Engineering

What Is Social Engineering?

Social engineering is a range of malicious activities undertaken by cybercriminals intended to psychologically manipulate someone into giving out sensitive information and data.

Under social engineering, a perpetrator initially investigates and examines the victim. Here, the victim’s basic background information is gathered, wherein the information may include potentially vulnerable entry points and security protocols required to carry out the attack.

The attacker then tries to perform subsequent actions that hamper the victim’s security practices by gaining their trust. Once the victim trusts the attacker, they may reveal sensitive information or grant access to critical and secure resources.

According to a 2020 report by Pulplesec, about 98% of all cyber attacks in the US used social engineering as the key tactic to break through security measures.

Social engineering specifically relies on human error rather than vulnerabilities in network systems, software, and operating systems. Mistakes committed by legitimate users are less predictable, so identifying them is harder than detecting malware-based intrusion.

In general, social engineering attacks primarily have two main objectives:

1. Sabotage: Cause harm or inconvenience by disrupting business or corrupting data.
2. Cyber Theft: Gain access to valuables, such as sensitive and critical information or money.

How does social engineering work?

Social engineering attacks generally occur when there is well-established communication between attackers and victims. The attacker prompts and motivates the user into compromising sensitive information, rather than explicitly employing a brute force attack for breaching the user’s data.

The social engineering attack life cycle provides criminals a reliable process that can easily deceive the victim. The steps involved in the social engineering life cycle include:

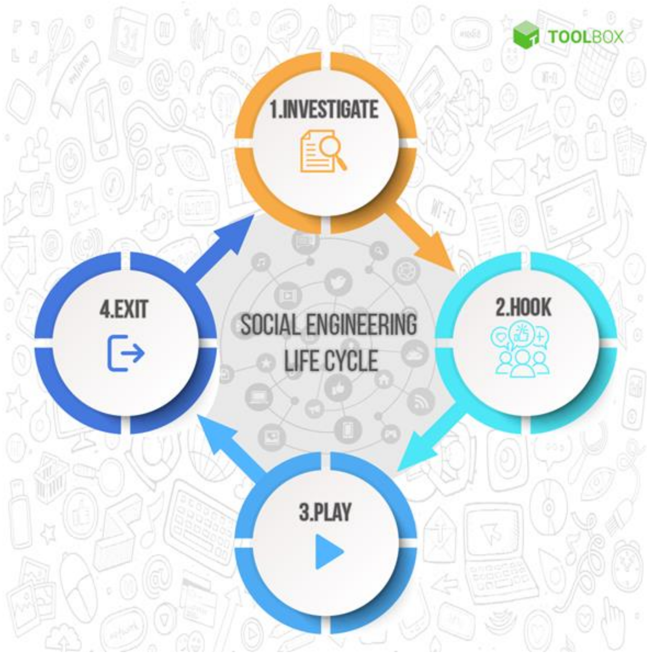


Figure: Social Engineering Lifecycle

Step 1. Target research: Preparation for an attack requires pre-planning from the perpetrator. Research time is invested in identifying the target's name, personal details, and background information. Based on this information, the attack methods/ channels are selected:

Step 2. Target hook: In this step, the attacker engages the target victim with a fabricated story that would be convincing, based on the information collected in the first step. The goal of the attacker here is to win the confidence of the victim.

Step 3. The attack: Once the target has obtained the necessary trust, the goal now shifts to extracting the information which is the real goal. Based on the intention, the attacker then uses the information or sells it.

Step 4. Exit: Once the attack's objective is complete, the window of engagement is then closed by the attacker, typically with the goal of avoiding any detection or suspicion. The attacker then attempts to cover their tracks and disappear to the best of their ability.

A common example of social engineering attempts made on senior citizens who may not have the required knowledge to identify digital foul play. An attack may be carried out using a combination of phone and email phishing techniques and convince the victim of passing out sensitive bank/ social security login details.

Common characteristics of social engineering attacks

Social engineering attacks pivot around the attacker's use of psychological tricks, such as persuasion or confidence. When the user is exposed to these tactics, they are more likely to take action than stay silent.

In most attacks, attackers mislead users by using an array of psychological manipulation techniques enlisted below:

1. Emotional manipulation

Emotional manipulation by exploiting heightened emotions gives attackers the upper hand in any kind of interaction with the victims. In such cases, when the victims are in an enhanced emotional state, they are more prone to taking irrational or risky actions. Emotions, such as anger, curiosity, excitement, fear, guilt, and sadness are often used in equal measure to convince the target victims.

2. Immediate action

Attackers tend to use time-sensitive opportunities or requests to fool users. The users may be motivated to compromise sensitive information or critical resources under the disguise of a serious problem that needs immediate action.

In some scenarios, users may be exposed to a form of a reward or prize that may disappear if they do not act immediately. Both these approaches tend to override the critical thinking or logical reasoning ability of the victim.

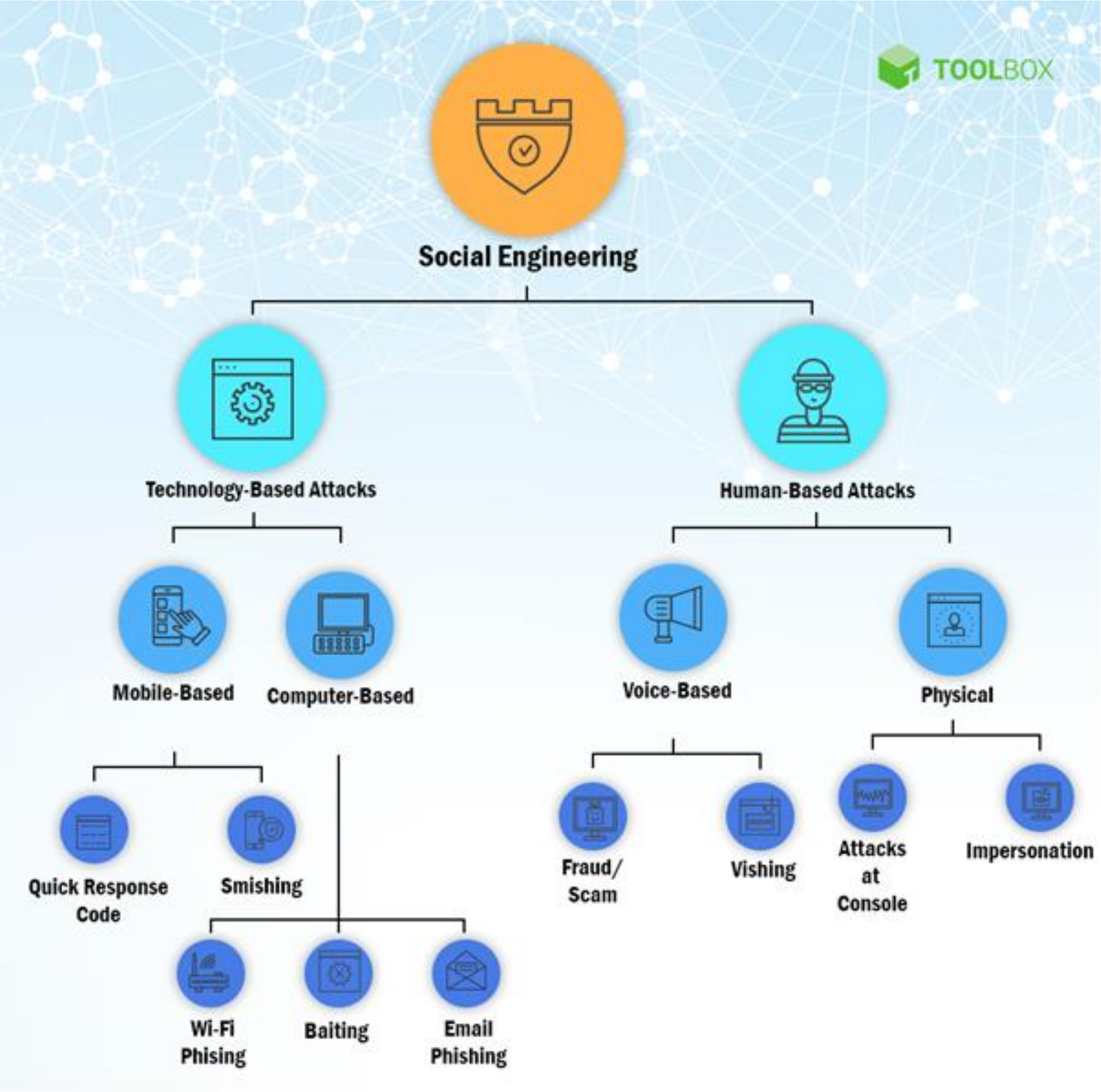
3. Trust

Social engineering attacks thrive on believability. Confidence and faith play a crucial role in these types of attacks as the attacker is aware of the fact that he is lying to the user. Attackers conduct substantial research on the target victim to cast a defined narrative that won't arouse suspicion.

4. Simplistic methods

Some exceptions to these common traits include simplistic methods that attackers use to gain network or system access. For example, a hacker at the common food court of a large organization building may "shoulder surf" users working on their tablets or laptops and try to access their sensitive information without sending an email or writing a line of virus code.

Types of Social Engineering



Types of Social Engineering Attacks

Social engineering attacks can be classified into two main categories:

1. Technology-based attacks

A technology-based approach tricks a user into believing that he is interacting with a ‘real’ computer system and convinces him to provide confidential information. For example, the user will get a popup window informing him that the computer application has had a problem and needs immediate fixing.

It will tell the user to reauthenticate a computer application to proceed. As the user proceeds to reauthenticate, the user provides his ID and password on the popup window itself. Once they enter the necessary credentials for authentication, the harm is done.

The hacker or the criminal who created the popup window now has access to the user’s ID and password and can, therefore, access their network and computer system.

Also Read: What Is Malware Analysis? Definition, Types, Stages, and Best Practices

2. Human interaction-based attacks

In a human interaction-based approach, the victim’s unawareness is exploited to attack the system or network. This is typically accomplished whereby the attacker pretends to be a person or authority the victim already knows while hiding their true identity.

3. Hybrid attacks

Hybrid attacks are the most common form of cyberattacks, where the attacker uses both technology and human interactions as platforms for conducting the social engineering attack.

For example, in a call to the helpdesk, a corporate social engineering attacker pretends to be a person of very high clearance/ authority within an organization and says that he/she has forgotten the password and needs to reset it immediately. In response, a nervous help desk personnel resets the password and give the newly set password to the person waiting at the other end of the call, rather than sending it via email. Having access to an email, the attacker now proceeds to send fake emails to other employees to coerce them into giving out further sensitive information.

In the above example, the attacker gained control of a technology portal (email), using a human interaction-based social engineering technique, then using the tech-based platform to conduct more social engineering attacks – all part of the same attack.

Also Read: What Is Ransomware Attack? Definition, Types, Examples, and Best Practices for Prevention and Removal

Key Techniques of Social Engineering Attacks

Social engineering assaults employ various techniques to gain access to the victim's sensitive data or network. These attacks come in various forms and can be carried out from any place where human interaction is involved. Let's take a look at them.

1. Baiting (Hybrid attack)

As the name suggests, baiting attacks harness a false promise to disorient a victim's greed or hunger. They trap users to steal their personal information or infect their systems with malware.The most common type of baiting involves the usage of physical media to disperse malware. For example, criminals leave the bait – typically malware-infected flash drives – in areas where there is a high probability of the potential victims seeing them. These areas include parking areas, elevators, washrooms, etc. The bait has a specific face value that can trick the victim into believing its authenticity. The external look of the bait can have a label that discloses an organization's payroll list.

Potential victims are generally convinced by the face value of the bait and, in turn, may insert it into a work or home computer system. This results in direct infection of the victim's computer as the malware gets installed on the victim's device dynamically.Baiting can be carried out in the physical as well as the online world, where online baiting consists of providing enticing ads that redirect users to malicious sites or motivate users to download a malware-infected computer application.

2. Contact spamming and email hacking (Hybrid attack)

In this type of attack, attackers hack into an individual's email or social media account to gain access to their personal contacts. Once hacked, the contacts are told that the individual has lost all credit cards. These contacts are then misled into transferring money to the attacker’s account. In another use case, a ‘must-see video’ is forwarded to the victim’s contacts, which is linked to malware or a keylogging Trojan.

3. DNS spoofing and cache poisoning attacks (Tech-based attack)

DNS spoofing manipulates a user’s browser and web servers to redirect the user to malicious websites when a legitimate URL is entered. Once infected with this attack exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.

DNS cache poisoning attacks categorically infect a user’s device with routing instructions to acquire multiple legitimate URLs to access fraudulent or malicious websites.

4. Phishing (Tech-based attack)

Phishing is one of the most popular social engineering attack types. Phishing scams employ email and text message campaigns to create a sense of urgency, curiosity, or fear in victims. They trick victims into disclosing sensitive information, clicking on malicious links, or opening attachments containing malware.

For example, attackers send an email informing the user of an online service that alerts them of a policy violation. The alert may ask the user to take immediate action, such as a password change.

This may include a link to an illegitimate website that is identical to its legitimate version. It may prompt the user to enter the correct credentials and a new password. Upon submission of the form, the information entered by the user is sent to the attacker.

In this type of attack, identical or near-identical messages are sent to all users through phishing campaigns. Hence, detecting and blocking such attacks are easier for mail servers having access to threat sharing platforms that are seemingly integrated within their framework.

5. Physical Breach Attacks (Hybrid attack)

Physical breaches involve attackers that appear in-person, identifying themselves as legitimate users to typically gain access to technical devices that are hard to breach.

Such attacks are commonly observed in organizational environments, such as government offices, businesses, or other enterprises. Attackers may pretend to be a representative of a known, trusted vendor for the company. In some cases, the attackers may even be recently fired employees who are holding a grudge against their former employer.

The attackers have a dubious identity but believable enough to avoid questions that can catch them in a spot of bother. Therefore, the attackers need to research at their end to avoid high-risk situations. So, if an attacker attempts a physical breach attack, they are guaranteed to have a highly valuable reward if successful.

6. Pretexting (Hybrid attack)

In a pretexting attack, the cybercriminal obtains sensitive information by using a series of lies. The scam is generally initiated by an attacker who misleads the victim into believing that they need sensitive information to perform a critical task.

The attacker initially establishes trust with the victim by impersonating co-workers, police personnel, bank and tax officials, or other individuals who have right-to-know authority. The pretexter then asks questions to confirm the victim’s identity. In this way, the pretexter gathers important personal data of the victim.

All kinds of sensitive information and data records are gathered using the pretexting attack. The sensitive information may include social security numbers, personal addresses, and phone numbers, phone records, bank records, etc.

7. Scareware (Hybrid attack)

In this type of attack, victims are bombarded with false alarms and fictitious threats. Users are tricked into thinking that their computer system is infected with malware, prompting them to install software that has no technical capability at all or, in some cases, the software is malware itself. Scareware is, therefore, referred to as deception software, rogue scanner software, and fraudware sometimes.

One example of scareware is a legitimate-looking popup displayed on the victim’s browser while surfing the web. The text on the popup may read “Your computer may be infected with harmful spyware programs”. The popup offers the victim two options — either to install the disclosed malicious tool (malware-infected) or to get redirected to a malicious site by clicking the pop-up window, thereby infecting the victim's computer.

Scareware is sometimes distributed via spam email that may highlight illegitimate warnings or offer users to buy worthless and harmful online services.

8. Spear phishing (Tech-based attack)

Spear phishing is a targeted version of the phishing scam. In this type of attack, an attacker identifies and chooses specific individuals or organizations. Once the target victim is identified, the scam then tailors messages based on the victim's characteristics, designation, and contacts to make their attack less conspicuous.

Spear phishing attacks are harder to detect and have better success rates. They may involve an attacker who impersonates an organization's consultant and sends an email to one or more staff members.

The mail is worded and signed exactly as the consultant usually does, thereby deceiving its recipients into believing that it's an authentic message. The message is convincing enough to prompt recipients into changing their passwords. In some cases, the message provides a link that redirects the recipients to a malicious page where the attacker captures their credentials with ease.

9. Vishing and Smishing (Hybrid attack)

Vishing and smishing are variants of phishing social engineering attacks, wherein one of the examples includes 'voice fishing', which means simply calling up and asking for data. In some cases, the attacker may act as a co-worker, for instance, impersonating an IT helpdesk personnel and asking for login information. Smishing attack uses text SMS to obtain sensitive information.

10. Watering Hole Attack (Tech-based attack)

Watering hole attacks infect popular websites with malware to target multiple users at the same time. In such attacks, the attackers perform a careful analysis to identify weaknesses in specific websites. They look for prominent vulnerabilities that are currently existing, not generally known, and patched. Such weaknesses are termed as zero-day exploits.

In some cases, the attackers may note that a site has not updated its framework to patch out known vulnerable issues and, in turn, infect it with malware. Website owners generally choose to delay software updates to keep software versions stable. They switch once the newer version has a proven track record of system stability. Attackers exploit this behavior to target recently patched vulnerabilities.

Impact of social engineering attacks

Information security is a significant ingredient for any organization ‘to continue to be in business’. If information security is not given importance, especially in the current scenario where the threat of cybercrimes looms in the background every day – any negligence or gap in security can bring an organization down.

In addition to financial losses, companies also lose reputation and goodwill in the market. Consider an example where a criminal gets access to the credit card information that an online vendor obtains from its customers.

In such a case, once the customer identifies that his credit card credentials have been compromised at an online site, the customer may not be willing to carry out any further business with the vendor, as they might consider the website an ‘insecure’ place. On the other hand, some customers may file lawsuits against the company, which may, in turn, affect the reputation of the company, thereby reducing the client count.

A well-known example is when PayPal, an online payment company, was at the receiving end of one such attack. The customers of PayPal received an email requesting the customers to re-enter their credit card data. PayPal reportedly had trouble with one of the computer systems.

However, the emails received by the customers looked genuine — the emails included PayPal logos, typefaces, security lock symbols, along with a link resembling the official PayPal link. As the account holders provided the credit card information, the attackers were able to misuse the data.

Cybersecurity experts have come to the conclusion that the majority of security violations are caused either by unhappy employees or non-employees who have legitimate system access because of their job in an enterprise. The FBI report says that nearly 80% of all social engineering attacks are caused by such authorized users.

In most scenarios, an honest individual acts like a criminal, wherein other employees do not view their activity with suspicion. The intruder further takes advantage of such a scene, wherein the individuals with a natural human tendency relax their guard on identifying that things appear secure from the outside.

Hence, social engineering attacks not only create financial losses for an organization but also hamper the organization's market reputation and goodwill.

Top 6 Social Engineering Threat Prevention Trends in 2020

Social engineers operate at a psychological level, where they manipulate human feelings, such as curiosity, anger, or fear, to work out schemes and draw victims into their planned traps. Therefore, users need to be aware and alert whenever they feel alarmed by a suspicious email, get inclined to an offer on a website, or come across stray digital media undertaking unknown sensitive activity such as collecting account credentials. Being alert and aware can help users protect themselves against most social engineering attacks in the digital realm. Here are the top six social engineering threat prevention trends in 2020.

1. Safe communication and account management habits

An individual is vulnerable to external threats only when he is exposed to some form of online communication or interaction – such interaction includes communication on social media, email, text messages, and in-person interactions. Following best practices can act as a firewall against social engineering attacks:

a) Do not click on links in emails or messages.

Always manually type a URL into the address bar, regardless of the sender. Also, take extra precaution in investigating to identify an official version of the URL under consideration. Do not engage with any URL that is not verified by you as official or is legitimate. Further, do not open attachments from suspicious sources.

b) Use multi-factor authentication.

The safety of online accounts is ensured when the user uses more than just a password to protect them. Multi-factor authentication adds additional layers to verify the user's identity upon login. Such factors can include user biometrics data like a fingerprint or facial recognition, or OTP passcodes sent via text message.

c) Use strong passwords.

Each user's password should be unique and complex, implying that the password should be difficult to guess. Try using various character types, such as uppercase, lowercase, numbers, and symbols. Further, prefer opting for long passwords.

d) Avoid sharing personal details.

Do not unknowingly expose answers to security questions or parts of a password while interacting with anything or anyone. Try setting up security questions that are memorable but inaccurate. By doing so, you'll make it harder for a criminal to crack the target account.

e) Cautious online friendships.

Although the internet is a great way to connect with people worldwide, it is also a common platform for social engineering attacks to flourish. So, watch out for red flags that indicate psychological manipulation or a clear abuse of trust.

2. Safe network use habits

Vulnerability can be exploited to its maximum stretch in compromised online networks. Hence, to safeguard users' data from getting tampered with and misused during social engineering attacks, it is important to take protective measures for any network that the user is connected to.

a) Do not allow strangers to connect to your primary Wi-Fi network.

Strangers at home or in the workplace should be allowed to access Wi-Fi via a guest Wi-Fi connection. Such an arrangement allows the main encrypted, password-secured connection to stay secure and interception-free. If any third party tries to “eavesdrop” for information, they won’t be able to access the activity you and others have kept private.

b) Use a VPN.

In scenarios where someone on the main wireless network (or wired, or cellular) finds a way to intercept traffic, a virtual private network (VPN) can keep such intruders out. VPNs provide services that allow users to keep their internet connection private over an encrypted “tunnel”. The connection is safeguarded against third-party intruders and eavesdroppers. Users’ data is anonymized so that it cannot be traced back to the user via cookies or other means.

c) Security of network-connected devices and services.

Securing network-connected devices, smart devices, and the cloud services associated with these devices is important. Protect the generally overlooked devices, such as home network routers or car infotainment systems, home theatres, etc. Data breaches on all these devices could spark personalization for a potential social engineering scam.

3. Safe device usage habits

Keeping devices safe is just as important as managing digital behaviors. Mobile phones, tablets, and other computing devices can be protected by following the below tips:

a) Comprehensive internet security software.

In scenarios when social attacks become successful, malware infections are a general outcome. To fight the rootkits, Trojans, and other embedded bots, it’s important to employ a sophisticated internet security solution to eliminate infectious intrusions and track their source.

b) Do not leave devices unsecured in public.

The best practice for a user at a workplace or any public setting is to always lock the computer and mobile devices so that no one gets ready access to these devices. In public places like airports, cafes, or commercial markets, always keep these devices in your possession.

c) Keep all your software updated.

Patch updates give software essential security fixes. As the updates are delayed or skipped, the software unknowingly exposes security holes for attackers to target. As criminals are generally aware of the characteristics of most computers and mobile users, you become a vulnerable target for socially engineered malware attacks.

d) Check for known data breaches of your online accounts.

Actively monitor new and existing data breaches for your online accounts, such as email addresses. Use security cloud services that provide a notification when the user's online account data is compromised. These cloud services further advise on taking action against data breaches.

4. Security awareness training

Healthy cybersecurity is aligned with human behavior. Social engineering dictates attacks by manipulating psychological behavior. Consider a phishing email, wherein the recipients are encouraged to click on an embedded link within the email or download a malicious file. Cybercriminals make the emails look like an authentic entity by using traits such as trust and a sense of urgency to disguise the nefarious email. Thus, ensuring that the entire workforce understands the various tricks followed by cybercriminals can be the best defense against social engineering.Social engineering protection begins by creating the right kind of awareness among individuals by educating them. If all the users are educated and alerted about such social assaults from time to time, then the collective safety of the society can be enhanced many folds. Hence, sharing the learned knowledge of these risks with co-workers, friends, and family can increase awareness among the masses, thereby allowing better remediation against any kind of social engineering attack.

5. Regular cybersecurity posture assessments

With each attack, cybercriminals tend to update and modify the social engineering techniques that they use to attack an environment. As deepfakes technology emerges in the security landscape – that manifests AI techniques for manipulating a voice or face, the social engineering attack techniques may also change.

Hence, advancing the cybersecurity posture assessment to help organizations strengthen their cybersecurity defenses by developing a comprehensive cybersecurity roadmap is of paramount importance. Cybersecurity posture assessment represents an insightful and useful first step for organizations looking to identify their current position in terms of security, currently missing components, and what needs to be done to increase their cybersecurity maturity level.

6. 24/7 monitoring practice

The security team's vigilance can be enhanced by testing and validating services that provide 24/7 monitoring. Businesses need to find a way to monitor their environments 24/7 cost-effectively if they wish to comply with regulations, secure their environment against cyberattacks or data breaches, or guarantee upward operational uptime.Monitoring involves using tools that can help detect problems on the network in real-time. Such tools may include techniques for performing behavioral analysis and some smart tools that may help to spot anomalies. Therefore, monitoring enhances the system's overall security by ensuring that software is kept up to date during all times and misconfigurations of servers are duly addressed.

How do I protect myself and my organization against social engineering?

While psychological attacks test the strength of even the best security systems, companies can mitigate the risk of social engineering with awareness training.Consistent training tailored for your organization is highly recommended. This should include demonstrations of the ways in which attackers might attempt to socially engineer your employees. For example, simulate a scenario where an attacker poses as a bank employee who asks the target to verify their account information. Another scenario could be a senior manager (whose email address has been spoofed or copied) asks the target to send a payment to a certain account.

Training helps teach employees to defend against such attacks and to understand why their role within the security culture is vital to the organization.

Organizations should also establish a clear set of security policies to help employees make the best decisions when it comes to social engineering attempts. Examples of useful procedures to include are:

- **Password management:** Guidelines such as the number and type of characters that each password must include, how often a password must be changed, and even a simple rule that employees should not disclose passwords to anyone--regardless of their position--will help secure information assets.
- **Multi-factor authentication:** Authentication for high-risk network services such as modem pools and VPNs should use multi-factor authentication rather than fixed passwords.
- **Email security with anti-phishing defenses:** Multiple layers of email defenses can minimize the threat of phishing and other social-engineering attacks. Some email security tools have anti-phishing measures built in.

How Social Engineering Attacks takes place?

Phishing scams are the most common types of Social Engineering attacks these days. Tools such as SET(Social Engineering Toolkit) also make it easier to create a phishing page but luckily many companies are now able to detect phishing such as Facebook. But it does not mean that you cannot become a victim of phishing because nowadays attackers are using iframe to manipulate detection techniques. The example of such hidden codes in phishing pages are cross-site-request-forgery “CSRF” which is an attack that forces an end user to execute unwanted actions on a web application.

Example: In 2018 we have seen a great rise in the use of ransomware which have been delivered alongside Phishing Emails. What an attacker does is they usually deliver an attachment with a subject like “Account Information” with the common file extension say *.pdf/.docx/.rar* etc. At which user generally click and the attacker’s job gets done here. This attack often encrypts the entire Disk or the documents and then to decrypt these files it requires cryptocurrency payment which is said to be “Ransom(money)”. They usually accept Bitcoin/Etherium as the virtual currency because of its non-traceable feature. Here are a few examples of social engineering attacks that are used to be executed via phishing:

- Banking Links Scams
- Social Media Link Scams
- Lottery Mail Scams
- Job Scams

Prevention

- Timely monitor online accounts whether they are social media accounts or bank accounts, to ensure that no unauthorized transactions have been made.
- Check for Email headers in case of any suspecting mail to check its legitimate source.
- Avoid clicking on links, unknown files, or open email attachments from unknown senders.
- Beware of links to online forms that require personal information, even if the email appears to come from a source. Phishing websites are same of legitimate websites in looks.
- Adopt proper security mechanism such as spam filters, anti-virus software, and a firewall, and keep all systems updated, anti-keyloggers.

An Insider Threat:

An insider threat is a category of risk posed by those who have access to an organization's physical or digital assets.

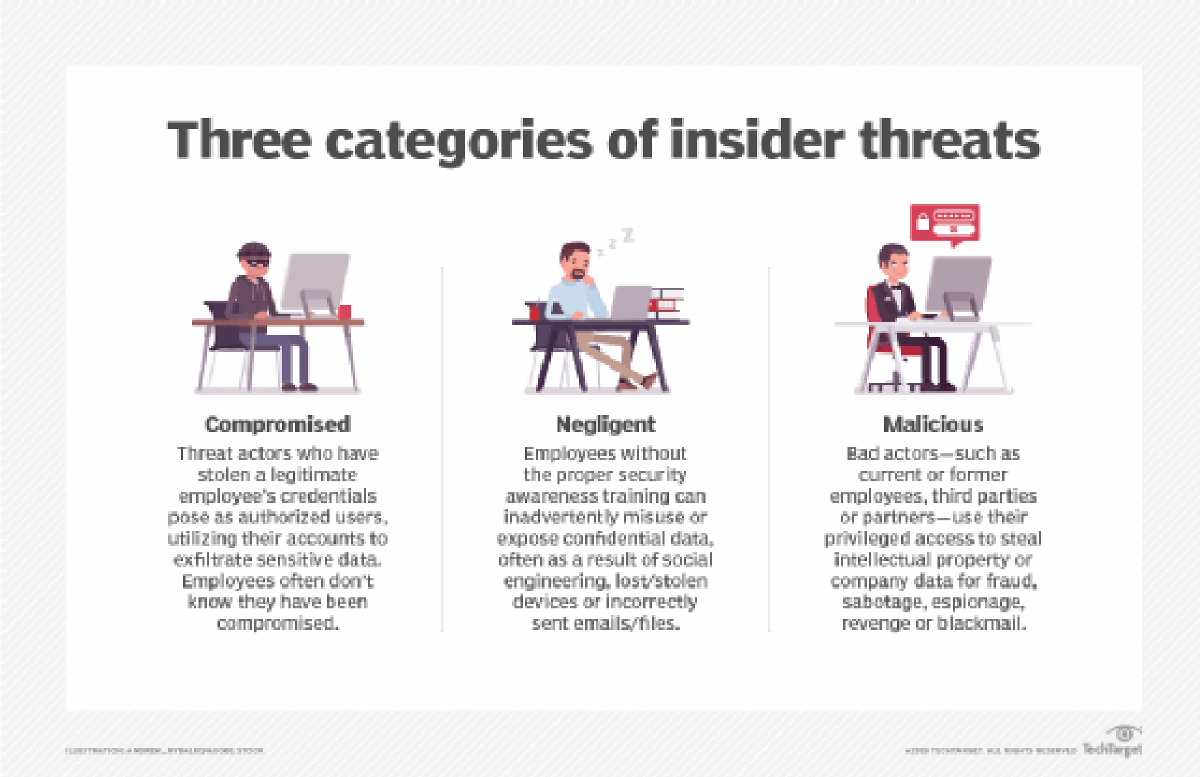
These insiders can be current employees, former employees, contractors, vendors or business partners who all have -- or had -- legitimate access to an organization's network and computer systems.

The consequences of a successful insider threat can take a variety of forms, including a data breach, fraud, theft of trade secrets or intellectual property, and sabotage of security measures.

What are the different types of insider threats?

Insider threats are defined by the role of the person who introduces the threat. The following are several examples of potential insider threats:

- **Current employees** could use privileged access to steal sensitive or valuable data for personal financial gain.
- **Former employees** could retain access to an organization's systems or pose a security threat by sabotaging cybersecurity measures or stealing sensitive data as a means of payback or personal gain.
- **Moles** are external threat actors who gain the confidence of a current employee to get insider access to systems and data. Often, they're from an outside organization hoping to steal trade secrets.
- **Unintentional insider threats** aren't caused by malicious employees, but rather, insiders who inadvertently pose a significant risk because they don't comply with corporate security policies or use company systems or data in a negligent manner. While unintentional, reckless behavior can open the door to external threats, like phishing, malware or endpoint



Three categories of insider threats

Compromised
Threat actors who have stolen a legitimate employee's credentials pose as authorized users, utilizing their accounts to exfiltrate sensitive data. Employees often don't know they have been compromised.

Negligent
Employees without the proper security awareness training can inadvertently misuse or expose confidential data, often as a result of social engineering, lost/stolen devices or incorrectly sent emails/files.

Malicious
Bad actors—such as current or former employees, third parties or partners—use their privileged access to steal intellectual property or company data for fraud, sabotage, espionage, revenge or blackmail.

Insider threats can be introduced through a range of sources but are classified in three categories.

Why are insider threats dangerous?

Insider threats can be hard to detect, even using advanced security threat detection tools. This is likely due to the fact that an insider threat typically doesn't reveal itself until the moment of attack.

Furthermore, because the malicious actor looks like a legitimate user, it can be difficult to distinguish between normal behavior and suspicious activity in the days, weeks and months leading up to an attack. With authenticated access to sensitive data, the insider exploit might not be apparent until the data is gone.

With few safeguards preventing someone with legitimate access from absconding with valuable information, this type of data breach can be one of the most costly to endure.

"Cost of a Data Breach Report 2020," a study produced by Ponemon Institute with IBM Security sponsorship, noted that "the average cost per lost or stolen record was $146 across all data breaches," but the cost went up to $150 for records containing customer personally identifiable information. The report also noted that 19% of companies experienced a malicious data breach because they were "infiltrated due to stolen or compromised credentials."

What are the warning signs that could indicate an insider threat?

To build awareness and improve detection of insider threats, there are several common signs that could indicate the presence of inappropriate insider activity in your organization:

- disgruntled employee behavior, such as displays of anger, exhibiting a negative attitude or talking about quitting;
- evidence of a user trying to circumvent access controls;
- dismantling, turning off or neglecting security controls, such as encryption or maintenance patches;
- frequently working late or in the office during off-hours when few others are present;
- violation of other corporate policies that may not be related to computer use;
- accessing or downloading large amounts of data;
- accessing -- or attempting to access -- data or applications that are not associated with an individual's role or responsibilities;
- connecting outside technology or personal devices to organizational systems or attempting to transmit data outside the organization; and
- searching and scanning for security vulnerabilities.

How can you defend against insider threats?

The Ponemon/IBM Security report identified several areas where modern organizations may be exposing themselves to insider threat incidents.

A lack of a baseline on nonmalicious, routine user behavior as a means of comparative analysis against suspicious behaviors was noted as a key shortcoming.

Another potential vulnerability resulted from poor identity management and access control protocols. An abundance of privileged accounts is an ideal target for social engineering and brute-force attacks, such as phishing.

To fill these gaps, there are two main paths forward: building awareness through proper training and using prevention and detection security measures.

Awareness and training program implementation

Employees should be properly trained on security risks so that they understand how to use the organization's systems safely and securely.

Security teams should specifically be trained on insider threat detection. Doing so can help them to better spot suspicious activity and prevent data loss or damage from insider attacks before they occur.

Detection and prevention security measures

In addition to improving employee training and awareness, most organizations have begun implementing insider threat programs that incorporate insider threat mitigation through detection, as well as prevention. This can be accomplished through compliance, security best practices and continuous monitoring.

Many cybersecurity tools can scan and monitor functionality to discover threats such as spyware, viruses and malware, as well as provide user behavior analytics.

Security controls can also be implemented to protect your data sources. Examples include encryption for data at rest, routine backups, scheduled maintenance and enforced two-factor authentication for password fortification.

Furthermore, identity management tools often automate user access revocation when an employee is terminated. These tools also provide greater control over what your employees have access to, so access to sensitive data sources can be limited.