Sri Lanka Institute of Information Technology

# Report of Social Engineering Attacks

Introduction To Cyber Security –IE2022

C.D Aluthge

IT22581402

Y2S1

Weekday - Group 1.1

Submission Date:

# Progress Overview -

In-depth examination of social engineering assaults, a pervasive and developing danger in cybersecurity, is provided in this report. It examines several social engineering assault types, their effects in the actual world, typical targets, and efficient preventative and mitigation techniques.

# Introduction -

A social engineering attack is a type of cybersecurity assault that depends on the psychological manipulation of people's behavior to get them to reveal confidential information, divulge login information, provide access to a personal device, or take other actions that undermine their digital security.

Since many attacks start on a personal level and rely on human error to continue the attack path, social engineering attacks constitute a serious danger to cybersecurity. Adversaries frequently succeed in accessing personal information or the endpoint itself by inspiring empathy, fear, and urgency in the victim. A path to enterprise-level attacks may also be opened up for adversaries if the device is linked to a corporate network or includes credentials for corporate accounts.

Organizations must be vigilant as cybercriminals develop ever-more cunning ways to deceive customers and employees.

# What is Social Engineering?

Peltier claims that the majority of social engineering attacks are carried out by outsiders who employ a range of psychological strategies to persuade the system user to divulge the data necessary for them to get access to a computer or network. This definition has grown into a catch-all term since 2006, referring to any attack that involves misusing someone's confidence and trust to carry out fraud, obtain illegal access, or coerce them into disclosing confidential information. These days, it also considers internal insider threats, including disgruntled employees. Social engineering is the hardest kind of attack to thwart; it cannot be prevented by technology and instead requires a robust information security architecture made up of regular vulnerability assessments and established norms and standards. It will go into further detail on how to protect yourself from social engineering attacks, which is a difficult undertaking without a universally workable solution.

As per the Verizon Data Breach Report, human involvement is involved in 85% of data breaches. Social engineering methods were used in the most common breach pattern. These numbers only included data breach incidents; they did not include fraud or information disclosure assaults against individuals. Social engineering is considered a bigger threat than other types of cyberattacks since it is a simple, cheap, powerful, and often successful technique for criminals to achieve their goals. The majority of victims—241,342—were reported to have been the result of Phishing, Vishing, Smishing, and Pharming, according to the Internet Crime Complaint Center's 2020 Annual Report, IC3. An antivirus company Research from a company called Barracuda looked at spear phishing attacks that happened between May 2020 and June 2021. They found that, on average, a corporation is the subject of 700 social engineering attempts annually. This study focused on tracking email-based attacks and did not include voice, SMS, or physical social engineering attempts.

## Evolution of the Social Engineering Attacks

### Social engineering in the digital age

Since the time of Charles Babbage (1791–1871), computational devices have existed, if not been used in daily life. Today, the phrase "Cyber Age" refers to more than simply computational tools; it also refers to the widespread usage of these tools in a setting where they are interconnected to form networks. In contrast to standalone computer machines like Babbage's Difference Engine, networks bring with them immediate security concerns. Consequently, even if the Cyber Age arguably

### today's social engineering

During the same time as confidence in social planning's performance began to erode, the idea of social engineering continued to be used more frequently within the cybersecurity community while keeping the fundamental qualities mentioned above. In fact, a review of 134 academic articles (published between 1990 and 2017) where authors established or supported a

> definition of "social engineering" revealed a bewildering variety of varied strategies weaved around the fundamental themes already mentioned: epistemic imbalance

## Type Of Social Engineering Attacks

Social engineering assaults involve multiple different attack vectors. These can be grouped together in many different ways, but the subdivision criteria are equally important. Person assaults and Person-Person via media attacks are the two primary types of social engineering attacks that Ivaturi and Janczewski distinguish between. The former describes an attack where the victim and attacker make direct physical touch, whereas the latter describes an occurrence where no physical contact occurs. The latter is further divided into speech, video, and text sections. Text-based attacks encompass online threats like malware, phishing, Smishing, and cross-site request forgery. Divide social engineering attacks into three categories: technological, social, and physical, depending on how they are executed. While assaults with a technical foundation use technology, like the internet, socially driven attacks use relationships to mentally manipulate victims. And last, physical attacks necessitate the attacker performing duties like going through trash looking for valuable documents by hand. This is important because, as the Mitre ATT&CK methodology points out, social engineering can also be used to enter a network and obtain access before pivoting to obtain additional access by technical or socio-technical methods. One such method for getting first access to a system is through phishing techniques.

## 1. Phishing Attack

Phishing is the most common type of social engineering assault. The three main objectives of most phishing scams are to: 1) collect personal information such as names, addresses, and Social Security numbers; 2) use shortened or misleading links to direct users to shady websites hosting phishing landing pages; and 3) exploit fear and a sense of urgency to elicit a quick response from the target. Phishing emails are never the same. Phishing attacks can occur through phone calls, social media, instant chatting, text messages (SMS), email, and more.

For example -

One Silicon Valley Bank-themed phishing campaign combined brand impersonation with a deceptive link and malicious attachment. (2023)

## 2. Pretexting Attack

Pretexting is a social engineering technique where an attacker fabricates a fabricated scenario or pretext to manipulate individuals into revealing information or performing actions they would not typically do. The attacker often pretends to be someone in authority, a trustworthy figure, or a person with a legitimate reason for the request. This technique is commonly used to gather sensitive information, such as personal data or login credentials, or to gain access to secure areas or systems.

For example -

In 2017, MacEwan University sent almost $9 million to a scammer posing as a contractor. The attacker asked staff to update their payment information through email. (2017)

## 3.Baiting Attack

In many ways, phishing and baiting are similar. The distinction is that baiting entices victims with the promise of an object or good. Using free music or movie downloads as an example, baiting assaults may use deception to persuade people to provide their login information. As an alternative, they may try to take advantage of people's natural interest by using physical media.

For example -

Back in July 2018, for instance, Cryptosecurity reported on an attack targeting state and local government agencies in the United States. The operation sent out Chinese postmarked envelopes with a confusing letter and a CD. The point was to pique recipients' curiosity so they would load the CD and inadvertently infect their computers with malware. (2018)

## 4. Quid Pro Quo Attack

A Quid Pro Quo attack is a sort of social engineering attack in which the attacker promises the victim a benefit or service in return for certain details or behaviors. Latin for "something for something," "quid pro quo" denotes a trade of benefits. In this situation, the attacker entices the victim to cooperate by promising them something desirable in exchange for sharing private information or allowing unauthorized access to systems or data.

For example -

One of the most common quid pro quo attacks is when fraudsters impersonate the U.S. Social Security Administration (SSA). These fake SSA personnel contact random people and ask them to confirm their Social Security Numbers, allowing them to steal their victims' identities. In other cases, detected by the Federal Trade Commission (FTC), malicious actors set up fake SSA websites to steal those people's personal information instead. It is important to note that attackers can use quid pro quo offers that are even less sophisticated. Earlier attacks have shown that office workers are more than willing to give away their passwords for a cheap pen or even a bar of chocolate.

## 5. Tailgating Attack

A Tailgating attack, also known as Piggybacking, is a physical security breach in which an unauthorized person gains access to a secured facility or area by following closely behind an authorized person. This type of attack exploits the trusting nature of individuals and the natural tendency to hold doors open for others, especially in corporate or institutional settings.

For example -

The attacker might impersonate a delivery driver and wait outside a building to get things started. When an employee gains security’s approval and opens the door, the attacker asks the employee to hold the door, thereby gaining access to the building. Tailgating does not work with specific security measures like a keycard system. However, in organizations that lack these features, attackers can strike up conversations with employees and use this show of familiarity to get past the front desk. Colin Greenless, a security consultant at Siemens Enterprise Communications, used these tactics to access multiple floors and the data room at an FTSE-listed financial firm. He could even set up shop in a third-floor meeting room and work there for several days.

## 6. CEO Fraud Attack

Finally, is Chief Executive Officer (or CxO) fraud. In this attack, cybercriminals first spend time gathering information about an organizational structure and key members of the executive team. In forgery, attackers use the credibility of the source of the request – such as the CFO – to convince an employee to perform financial transactions or provide sensitive and valuable information. A CEO fraud, also known as executive phishing or business email compromise (BEC), is a spear-phishing attack.

For CEO fraud to be effective, an attacker familiarizes themself with the org chart and general purpose of the organization. After identifying key players and targets within the company, an attacker gains control of an executive’s email account through a hack.

Impersonating the CFO, for example, the attacker will contact someone in the accounting or purchasing team and ask them to pay an invoice - one that is fraudulent, unbeknownst to the employee. This request will typically come with a sense of urgency as attackers know time is money and the longer it takes to complete the request, the higher the chance that the employee will catch on.

For example -

According to the FBI, BEC attacks cost organizations more than $43 billion (about $130 per person in the US) (about $130 per person in the US) (about $130 per person in the US) (about $130 per person in the US) (about $130 per person in the US) (about $130 per person in the US) (about $130 per person in the US) between 2016 and 2021.

## 7. Spear Phishing Attack

A spear phishing assault is a type of targeted phishing attack in which thieves concentrate their efforts on a particular person or business. Spear phishing is highly individualized and designed to target the targeted recipient's vulnerabilities, preferences, and relationships, in contrast to generic phishing assaults that spread their net widely. The intention is to trick the receiver into disclosing personal data, clicking on nefarious links, or downloading malware.

For example -

83% of UK businesses that suffered a cyber-attack in 2022 reported the attack type as phishing.

## 8. Vishing (Voice Phishing) Attack

The term "Voice Phishing," also known as "Vishing," refers to a type of social engineering attack in which criminals utilize phone calls to trick people into disclosing sensitive information such as passwords, credit card details, personal identification numbers (PINs), or other private information. Like classic phishing attempts done via email, vishing attacks use voice communication to trick and take advantage of their victims.

For example -

veer 59.4 million people (about twice the population of Texas) in America fell victim to vishing in 2021 The average reported loss to vishing increased 43% in 2021 59% of Americans received scam calls related to COVID-19 in 2021 Youngsters between the ages of 18-44 years are more susceptible to vishing attacks An average American received nearly 31 spam calls a month in 2021 Peru recorded more than 12 million spam calls in October 2021 Mexican people received over 3.2 million spam calls in October 2021

## 9. Impersonation Attack

An impersonation attack is a type of social engineering in which the attacker poses as someone they are not to trick people or organizations into doing something they would not normally do or disclosing sensitive information. Attacks involving impersonation can take many different shapes, and the perpetrator may pass for a variety of people or organizations, including CEOs, coworkers, and trusted individuals.

For example -

Toyota: In 2019, Toyota Boshoku Corporation, a European subsidiary of the Japanese giant, fell victim to a $37 million BEC fraud. While Toyota did not reveal details about the exact method used by the scammers, it is evident that the scammers used social engineering to impersonate executives and targeted specific individuals to comply with their requests.

Google and Facebook: Between 2013 and 2015, the two tech behemoths lost $121 million to a Vendor Email Compromise (VEC) attack. The perpetrator set up a fake company with the same name as an actual hardware supplier and created fake contracts and legal letters to get banks to accept payments. They then sent invoices to Facebook and Google, which were duly honored.

Unnamed European corporate victim: In March 2019, criminals used AI-based Deepfake Voice technology to impersonate a company’s CEO’s voice. A phone call was made to the CEO of a

British subsidiary, demanding an urgent €220,000 payment. The victims' insurance provider declined to name the victims.

## 10. Reverse Social Engineering attack

A social engineering attack is called reverse social engineering (RSE). The attack's goal is the same as a standard social engineering attempt, but its methodology is entirely different. In this person-to-person attack, the victim is approached directly to coerce them into disclosing private information. The hacker typically contacts the target through emails and social media platforms, employing various deception techniques and posing as a generous donor or knowledgeable security staff to persuade them to grant access to their system or network. Even though it may appear archaic and ludicrous, this tactic has been successful, especially when the victim's system or network exhibits evidence of compromise.

## Difference between social engineering and reverse social engineering?

Typically, the attackers in social engineering attacks approach their targets. In contrast, the victim inadvertently approaches the attacker in reverse social engineering attempts.

## 11. Honey trapping attack

A common investigation technique is called "honey trapping," which involves using romantic or sexual relationships for monetary, political (including state espionage), or other purposes. The honeypot or trap entails contacting a person who has the knowledge or resources that a group or individual needs; the trapper will then try to entice the target into a false relationship (which may or may not include actual physical involvement) to gain access to the target's information or leverage over them.

When dating websites are used to contact a victim, this practice is called a "honey trap".

Wives, husbands, and other partners frequently hire private investigators to set up a honeypot when the "target" or subject of the inquiry is suspected of having an illicit relationship. The phrase is occasionally applied to the process of staging an affair so that embarrassing images can be taken for blackmail purposes. A honey trap is primarily used to gather data related to the honey trap. Drug smuggling and drug addiction are both achieved through honey traps.

For example -

Beijing said Monday that a US citizen jailed for life for espionage lured Chinese officials into bugged hotels and used "honey traps" to blackmail them into spying for Washington.

## 12. Eliciting Information

Eliciting information is a social engineering tactic in which a perpetrator uses techniques to covertly get sensitive or priceless information from people or organizations. Elicitation relies on swaying discussion and contact to elicit information without arousing suspicion, as opposed to more overt techniques like phishing or impersonation. Attackers frequently employ this method to learn more about how an organization operates, collect private information, or take advantage of weaknesses.

## 13. Psychological manipulation

The practice of persuading someone to divulge private information or do actions that could lead to a security breach is known as social engineering.

These assaults employ several strategies to dupe victims into disclosing private information or installing dangerous software on their devices. Social engineering attacks have increased in frequency and sophistication with the development of digital technology and social media, creating a significant cybersecurity threat.

Attacks using social engineering take advantage of human emotions, anxieties, and weaknesses. Hackers use psychological manipulation strategies to persuade someone to do certain behaviors or divulge private information. These methods might be as straightforward as instilling a sense of urgency or as intricate as developing a close bond with the victim.

## 14. Pharming

Pharming[a] is a cyberattack designed to trick users into visiting a phony website by downloading and installing a malicious application on their devices. [Reference needed] Pharming can be carried out either by altering the hosts file on the victim's machine or by taking advantage of a flaw in the DNS server program. Computers called DNS servers oversee converting Internet names into their corresponding IP addresses. Some people use the term "poisoned" to describe compromised DNS servers. Instead of using a corporate business server, phishing involves unprotected access to a computer, such as changing a customer's home PC.

The phrases "farming" and "phishing" were neologized to create the term "pharming". An example of a social engineering assault is phishing, which aims to get access credentials such usernames and passwords. Both phishing and pharming have been employed in recent years to gather information for online identity theft. Businesses that host e-commerce and online banking websites are now extremely concerned about pharming. To counter this grave threat, sophisticated anti-pharming methods are necessary. Pharming is not something that antivirus and spyware removal tools can guard against.

## 15. Watering Hole Attack

A predator striking its prey as it stops by a watering hole to drink is one example of how watering hole attacks, also known as watering hole phishing, got their name. Imagine a lion lurking at a well-known watering place on the savanna, ready to strike when an unwary antelope stoops to drink. Although the antelope is a simple target, other animals of different kinds frequently gather at the watering hole.

When we describe a watering hole attack in the context of cybersecurity, the rationale behind this comparison becomes obvious. Threat actors seek to attack their targets where they gather, typically on websites that the target frequently visits. Given how frequently they use that website, the target rarely considers its security, making them open to unexpected attacks from a variety of sources.

The idea behind watering hole attacks is simple, but it is also crucial to comprehend how cyberattacks carry them out and make money from them. Watering hole attacks typically consist of four steps that are designed to track, examine, and use a variety of web-based exploits.

For example -

2012: Hackers infected the American Council on Foreign Relations (CFR) website through an Internet Explorer exploit. Interestingly, the watering hole only hit Internet Explorer browsers that were using certain languages.

2013: A state-sponsored malware attack hit Industrial Control Systems (ICS) in the United States and Europe, targeting defense, energy, aviation, pharmaceutical, and petrochemical sectors.

2013: Hackers harvested user information by using the United States Department of Labor website as a watering hole.

2016: Researchers found a custom exploit kit targeting organizations in over 31 countries, including Poland, the United States, and Mexico. The source of the attack may have been the Polish Financial Supervision Authority’s web server.

2016: The Montreal-based International Civil Aviation Organization (ICAO) is a gateway to all airlines, airports, and national aviation agencies. By corrupting two of ICAO’s servers, a hacker spread malware to other websites, leaving the sensitive data of 2000 users and staff members vulnerable.

2017: The Not Petya malware infiltrated networks across Ukraine, infecting website visitors and deleting their hard drive data.

2018: Researchers found a watering hole campaign called Ocean Lotus. This attack hit Cambodian government websites and Vietnamese media sites.

2019: Cybercriminals used a malicious Adobe Flash pop-up to trigger a drive-by download attack on a dozen websites. Called Holy Water, this attack hit religious, charity, and volunteer websites.

2020: American information technology company SolarWinds was the target of a watering hole attack that took months to uncover. State-sponsored agents used the watering hole attack to spy on cybersecurity companies, the Treasury Department, Homeland Security, etc.

2021: Google’s Threat Analysis Group (TAG) found widespread watering hole attacks targeting visitors of media and pro-democracy websites in Hong Kong. The malware infection would install a backdoor on people using Apple devices.

## 16. Credential harvesting

Organizations are more vulnerable to harmful cyberattacks like credential harvesting because of the digital transition. Credential harvesting is the practice of attackers posing as reputable websites or organizations to get user credentials, including usernames, passwords, and credit card information. One of the most common cyberattacks nowadays is credential harvesting, and it keeps getting more advanced. Phishing attacks have evolved to be more targeted and convincing, and they now use a variety of methods to get private and sensitive data.

To safeguard themselves against connected cyber-attacks, organizations must remain ahead of such new dangers and modify their security procedures. A cyberattack known as "credential harvesting" targets sensitive and confidential information, including other user digital credentials (such one-time passwords, authentication tokens, etc.). In other terms, it is a malicious tactic employed by attackers to steal sensitive information from unwitting victims, such as usernames, passwords, banking information, and credit card numbers. Using phishing frauds, where thieves send emails that pretend to be from reliable sources to persuade the victim to submit their credentials, credentials are often harvested. When they get access to a user's system through malware, they can sometimes obtain credentials without the user's knowledge. Because these criminals have improved their methods, this kind of attack has increased in frequency in recent years.

## 17. Job Recruitment Scams

Many people would like to work from home and earn money. Scammers are aware of this, so they post advertising, frequently online, claiming to have employment opportunities where you can work from home and earn thousands of dollars each month with little time and effort. The work could involve anything from product reshipping to selling to acquaintances. Scammers will occasionally promise you the chance to work for yourself, launch your own company, or set your own hours to pique your interest.

However, you end up spending your money on pointless beginning kits, so-called training, or certifications rather than earning money. You might also discover that someone has used your credit card without your consent, or you might fall victim to a fake check scam in which you deposit a check from your new employer, who then requests that you send back some money because of a "overpayment," but the check ultimately bounces and the bank demands that you pay back the full amount of the fake check while the con artists keep the real money you sent them.

## 18. Tech Support Scams

Tech support frauds are dishonest schemes in which hackers pretend to be legitimate tech support agents or businesses to trick people into thinking that their computers or other electronic devices have serious problems, viruses, or malware. The con artists then make an offer to help address the alleged issues, frequently asking for remote access to the victim's computer and payment for their services. Tech support frauds may lead to property damage, identity theft, and the compromise of private information.

Tech support frauds can be traced back to Mumbai, Kolkata, or other locations in India. Around 2008, the first reports of these tech support fraud (TSS) arose, and they have steadily gained ground since then.

2013 saw a sharp increase in TSS cases as con artists started to employ malicious advertising to spread false alarms. The Internet Crime Complaint Center, often known as IC3, released a PSA about the new digital twist on tech support swindles a year later to inform Internet users, encourage the public to report incidents, and advise them to exercise caution.

Digital tech support frauds became well known not long after, and big tech corporations started to defend themselves. Microsoft openly sued several businesses, including one in India, in December 2014, claiming that they had misrepresented themselves as offering technical assistance services connected to Microsoft. Additionally, the FTC began to make some significant strides in 2015 in its efforts to aid and defend both consumers and IT corporations. They announced the closure of many techs support con artists who impersonated Apple, Microsoft, and Google Tech

Support and took close to $17 million from consumers in November of that year.

But the battle has only just begun. Tech support frauds have developed since the FTC's first significant victory, and they continue to defraud customers of millions of dollars each year.

## 19. Ransomware

Malicious software, or malware, known as ransomware, is created to prevent users from accessing a computer system or certain data unless a ransom is paid. Phishing emails, malicious advertising, accessing infected websites, and vulnerability-based attacks are all ways that ransomware spreads. Data breaches, data leaks, intellectual property theft, and downtime are all consequences of ransomware attacks. A few hundred to several hundred thousand dollars can be demanded as ransom. ability to be paid in digital currency like Bitcoin. Several online frauds let hackers access your computer so they can install ransomware, including social engineering and phishing: Ransomware spreads by persuading victims to open an email attachment that seems like it is from a friend or superior. Malvertising: To distribute ransomware, malvertising requires an infected iframe or invisible element. The iframe takes users to a page that launches malicious software or an exploit kit to carry out an unauthorized drive-by download. Vulnerabilities: Ransomware that is more aggressive, like WannaCry, takes advantage of flaws to automatically infect systems. Ransomware can encrypt all or certain data once it has been installed. A ransom message that follows the initial ransomware infestation explains why the files are inaccessible. For the decryption key to unlock their files, the victim must send a ransom.

The victim's computer has been locked by law enforcement, according to other ransomware, because it contains pirated software or pornographic material. A fine must then be paid to unlock the computer.

Another type of ransomware is leakware, often known as Dox ware. Threatening to expose private information on the victim's hard drive.

This type of ransomware carries some risk. resulting in the disclosure of personally identifiable information (PII) or large data breaches.

# Impact of Social Engineering Attacks

Attacks using social engineering are particularly risky because not everyone needs to be the target. One person who was successfully duped may leak enough information to start widespread attacks and cause great harm to the company.

These attacks use the element of human error to trick unsuspecting users into downloading malware, disclosing passwords, sending money, clicking on phony adverts or spam links, or buying goods, among other things. Successful social engineering attacks may result in illegal access, service interruption, data theft, reputational harm, malware, ransomware, and other attacks. The preparation/reconnaissance stage of social engineering is: The attacker chooses victims and invests a lot of time and money to learn crucial details about them. The attacker also compiles all pertinent background data regarding them, including potential points of entry, security flaws, etc. They will choose the attack strategies considering this.

Stage of deception or infiltration: The attacker interacts with the targets to win their confidence. To entice their prey, they concoct tales or offer persuasive justifications. The attacker attempts to exert control over the conversation by appealing to the target's vulnerabilities (fear, shame, sadness, curiosity, etc.). To further the attack and influence the victim to do their bidding, they take advantage of the unwitting victim. After the user has completed the desired action, the attacker will disengage, bringing the interaction to a natural end. They will also eliminate virus traces, hide their trails, etc. The assault lifetime may last just one phone call, one email exchange, or several months on social media talks. They might or might not entail voice or face-to-face communication.

Did you know that more than half of all businesses become a target of a social engineering or spear phishing attack every year? The figure is truly scary and in today’s world, social engineering is one of the biggest threats both small and large businesses face in the cybersecurity world.

## What can happen to you if you are attacked?

### 1.Financial losses due to social engineering attacks are listed below -

The amount of money the company loses as a direct result of a social engineering attack is the only effect of hacker attacks that everyone is aware of. This sum can range from $20,000 to millions of dollars depending on the size of your business and the attacker's avarice.

### 2.SOCIAL ENGINEERING CYBER ATTACK-RELATED PRODUCTIVITY LOSS

The normal course of business is severely disrupted by any successful cyberattack. To cope with the breach, the IT team and numerous management-level employees must put off other tasks. Additionally, all employees must be informed about the hack and given training on how to avoid a similar attack in the future. The employees' workload is interrupted by all of this, which sharply reduces productivity.

## 3.THE COST OF REHABILITATION FOLLOWING A SOCIALISTIC ENGINEERING ATTACK

The recovery cost, which includes the money required to hire an incident response team, buy software that will stop a similar attack from happening in the future, and deal with customers whose data was stolen during the attack, is another typical expense linked to spear-phishing attacks.

## 4.BUSINESS DISRUPTIONS ARE CAUSED BY CYBER-ATTACKS

This social engineering effect is comparable to productivity loss, except it assesses how the hack affects your supply chain and customer satisfaction scores. Your company can incur interruption in product manufacture, shipping, or other operations because of a successful hacking attack that interferes with your regular business operations. You can lose clients or even suppliers because of this. Additionally, after the incident, your bank and insurance provider may both want to check up on your business' cybersecurity procedures.

# How to detect social engineering attacks?

The prevalence of social engineering assaults has increased as more businesses use third-party, mission-critical technologies. According to Verizon's yearly study, 82% of successful data breaches are still caused by people. This vulnerability is still being used by threat actors and social engineers, and the damage caused by these attacks is still quite expensive.

Bad actors obtain sensitive information and priceless resources by tricking others into violating security protocols. They can infiltrate and take advantage of an enterprise's networks by utilizing numerous attack methods like spear phishing, business email compromise, and malware delivery.

Such attacks can be recognized in many ways. Generic signatures and greetings, suspicious attachments, and poor grammar and formatting can all be signs of ongoing social engineering operations. Executives and staff must be educated on the best practices for preventing social engineering assaults.

To acquire unauthorized access to systems, networks, or physical locations or for financial gain, social engineering is an attack vector that "heavily relies on human interaction and frequently involves manipulating people into breaking normal security procedures and best practices."

Social skills are used by the attacker in social engineering attacks to gather or compromise information about a company or its computer systems. An attacker can present themselves as unassuming and reputable, offering credentials to prove their identity as a new employee, repairperson, or researcher, or they might even make such claims.

They might be able to gather enough information, nevertheless, by probing the network of an organization with queries.

- Baiting

The attacker leaves a physically compromised device, like a USB flash drive, in a place where it is likely to be found. The malware is inadvertently installed when the target picks it up and installs it inside their computer.

- Phishing

when a malevolent entity sends what appears to be a legitimate email but is actually fraudulent and usually purports to be from a trustworthy source. The message's objective is to trick the recipient into clicking on a harmful link or divulging personal or financial information.

- Whaling

A particular type of spear-phishing attack targets high-profile workers, like the chief financial officer or chief executive officer, in an attempt to trick the targeted person into providing vital information.

- Vishing

This is one social engineering threat that grew out of regular phishing. The technique of employing social engineering to get financial or personal information over the phone from a target is known as vishing, sometimes known as voice phishing.

- Smishing

a social engineering method that uses text or SMS messaging. Text messages may contain links that open a browser window, an email message, or a phone call when clicked. These links can also connect to websites, email addresses, or phone numbers.

- Pretexting

One party deceives the other in order to obtain secret information. In a pretexting scam, for example, the attacker can say they need personal or financial data to confirm the recipient's identity.

- Scareware

This comprises tricking the victim into thinking that malicious software is on their computer or that they have inadvertently downloaded illegal content. The attacker then poses a fix for the fictitious issue in an attempt to trick the victim into downloading and installing the malware.

- Watering hole

The attacker attempts to infect websites that a certain group of users is known to visit and trust in order to get access to the network.

- Quid pro quo

In a social engineering attack, the attacker purports to be offering something in return for the target's assistance or information. For example, while phoning random people within an organization, a hacker may pose as a technical support person responding to a ticket. Eventually, the hacker will find someone who is experiencing technical difficulties, and they will pose as helpers for that individual. This exchange can be used by the hacker to steal password information or to get the target to enter commands to launch malware.

- Honey trap

In this attack, a social engineer poses as an attractive person to interact with a target online, establish a phony relationship, and then utilize that relationship to obtain private information.

- Pharming

This type of online fraud is a cybercriminal installing malicious malware on a computer or server, which then automatically directs users to a phony website where they could be tricked into providing personal information.

# Strategies to mitigate social engineering attacks.

Tackling social engineering is an essential part of any information security regime.

## 1. Personnel Education and Training

Understanding social engineering risks and how to handle them is the first step in safeguarding a business from them. In order to protect the company in the event that anti-phishing software and other measures fail to successfully ward off threats, it is imperative that employees are made aware of what a phishing effort looks like and what they should do when confronted with one.

Employers can accomplish this through promoting awareness among staff members, confirming their expertise, and providing ongoing education. In the training process, it might also be beneficial to occasionally test staff understanding by sending out a phishing email.

Users should know not just what not to do, but also what to do in the event of a phishing effort. Users should constantly be cautious and aware of the telltale indicators of phishing attempts, which include:

Shortened and error-filled URLs.

Unsecured HTTP websites.

Webpages with broken images and links.

Suspicious emails requesting sensitive information or not following overall protocol.

## 2. Anti-Phishing Software

Anti-phishing software should be incorporated into an organization's whole IT infrastructure to prevent social engineering attacks.

Although lists of popular phishing websites are freely shared on websites, these lists shouldn't be used to create anti-phishing software. This is due to the fact that patient zero will never go away and these places unfortunately change on a regular basis. Employee productivity will suffer as a result of the software's pointless blocking of access to other websites because it has no way of distinguishing which websites are phishing sites and which are genuine.

## 3. Solutions for Browser Security

The best protection against social engineering and other phishing attacks is to secure the browser as a whole. Good solutions prevent attacks before they become too late and protect users against a variety of attacks, not only phishing scams. Robust browser security programs need to enforce compliance by monitoring runtime telemetry and operating independently of other third-party feeds.

The ability of browser security solutions to thwart all browser assaults, including exploitation, social engineering attempts, and online application vulnerabilities, is crucial. They must also have the ability to halt rules infractions by users. Because an enterprise's security level is determined by the weakest link in its multi-layer defense, the browser must be the most secure element of the organizational supply chain.

## Successful mitigation of cyber-attacks and security breaches

Organizations must successfully mitigate cyberattacks and security breaches in order to safeguard their data, operations, and reputation. A few case studies of effective mitigation initiatives are provided below:

- Sony Pictures Entertainment (2014):

Attack: In 2014, Sony Pictures experienced a significant cyberattack that led to the loss of private information and the disclosure of employee records, unreleased films, and private correspondence.

Mitigation: In order to rapidly address the issue, Sony Pictures called in law enforcement and cybersecurity specialists. After stopping the attack and isolating the compromised systems, they started to rebuild and secure their network. The business maintained open lines of communication with both the public and its staff.

Conclusion: Despite the fact that the attack resulted in significant damage, Sony Pictures was able to confine the breach, stop more data loss, and eventually recover from the disaster thanks to their prompt response. It emphasized how critical a prompt and well-planned response is.

- Target Corporation (2013):

Attack: In 2013, there was a data breach at Target, resulting in the theft of millions of consumers' personal and credit card details by cybercriminals.

Mitigation: Target acted quickly to halt illegal access, cooperate with law enforcement, and contact impacted consumers in order to minimize the incident. The business made significant investments to strengthen its cybersecurity defenses as well.

Result: By strengthening its cybersecurity architecture and implementing a prompt response to the breach, Target was able to win back customer trust and avert future occurrences of this kind.

- Maersk (2017):

Attack: In 2017, the Not Petya ransomware outbreak crippled the IT systems of the multinational shipping corporation Maersk and caused disruptions to its operations throughout the globe.

Mitigation: In order to contain the infection and isolate the impacted systems, Maersk had to completely rebuild its IT infrastructure. They worked together with government organizations and cybersecurity companies to look into the incident and get their data back.

Result: Although the attack had a major effect on Maersk's operations, they were able to progressively restore services and restart regular business operations because of their prompt and thorough response.

- Equifax (2017):

Attack: In 2017, a data breach at the large credit reporting company Equifax resulted in the exposure of over 143 million people's private information.

Mitigation: In response, Equifax hired cybersecurity specialists, started a thorough investigation, and put safeguards in place to stop similar incidents in the future. They provided affected people with free credit monitoring services.

Outcome: Equifax's efforts led to the identification and arrest of the hackers responsible for the breach. While the incident had severe consequences, Equifax's mitigation measures helped them address the immediate issue and improve their security practices.

These case studies demonstrate the importance of timely and well-coordinated responses to cybersecurity emergencies in addition to continuous efforts to strengthen cybersecurity defenses against future attacks. Every company strengthened its security posture by applying the valuable insights it learned from its distinct circumstances.

## Emerging trends and future threats in social engineering attacks

### Threats And Trends in Social Engineering in the Future

### Individualized Attacks

Without a doubt, social media has streamlined our lives. Social media helps us stay in touch with our loved ones and share our lives. However, the regular dissemination of personal data increases the opportunity for online criminals.

Attackers are constantly looking for ways to get access to people's personal or professional accounts so they may track their social media activity and create phishing emails or phone frauds using the personal information they have obtained. For instance, the names of one's children and their childhood memories, together with all other personal information shared on social media, are frequently employed in account logins.

When sharing and creating anything on social media, you should always have your accounts set to private. Limit the number of friend requests you accept from people you do not know.

## Swapping SIMs

Enabling two-factor authentication wherever possible is one of the top recommendations for cyber security from respected industry professionals. However, a developing practice known as "SIM swapping" renders this security advice meaningless. Attackers are utilizing SIM swapping, a social engineering technique, to access the victim's account. Attackers in this scenario are users whose accounts use two-factor authentication to enter the one-time passcode delivered to their phone. Once the passcode is revealed, cybercriminals can use it to their advantage to intercept any calls and texts that are meant for the victim.

This enables cybercriminals to obtain all login credentials for accounts and access a victim's personal accounts. You must be particularly vigilant about paying attention to the websites you use to get into personal accounts, even if you should still implement two-factor authentication whenever it is possible.

## Deepfakes

Deepfake technology is currently a major source of worry for the cyber security sector. It takes a combination of machine learning and artificial intelligence to modify a video, photo, or audio clip with malicious intent. These mediums are used to trick victims into providing personal and sensitive data.

This trend began to gain traction in 2017. It was initially used as a tool to edit the faces of celebrities and other people onto pornographic recordings to make it appear as though they were the ones being filmed.

Some people worry that deepfakes could be used to modify political photos and videos in advance of the 2020 presidential election. Experts in cyber security are concerned about this new trend because of the potential for deepfakes to trick people into disclosing their personal information.

# References

Assman, B. (2023) *Social Engineering Threat Trends 2023*, *Convergence Networks*. Available at: https://convergencenetworks.com/blog/social-engineering-threat-trends-insights/ (Accessed: 10 October 2023).

Ekta (2023b) *Social Engineering Emerging Trends and threats 2023*, *Identity Management Solution & MSSP Company*. Available at: https://sennovate.com/the-future-of-social-engineering-emerging-trends-and-threats/ (Accessed: 10 October 2023).

Safeguard Cyber (2023) *Identify and prevent social engineering attacks*, *Safeguard Cyber*. Available at: https://www.safeguardcyber.com/identify-prevent-social-engineering-attacks (Accessed: 10 October 2023).

Levin, A. (2023) *Social engineering attacks: 3 strategies to mitigate risk*, *Techopedia*. Available at: https://www.techopedia.com/social-engineering-attacks-3-strategies-to-mitigate-risk/2/34899 (Accessed: 10 October 2023).

Irwin, L. (2022) *5 ways to prevent social engineering attacks*, *GRC eLearning Blog*. Available at: https://www.grcelearning.com/blog/5-

ways-to-mitigate-social-engineering-attacks (Accessed: 10 October 2023).

Sitelock.com - https://www.sitelock.com/blog/the-impact-of-social-engineering/

Manager (2021) *What is the impact of social engineering attacks? - hack control - cybersecurity consulting company, cyber security, Penetration Testing, security audit, Brand Protection, Anti phishing, blockchain audit, Hack Control*. Available at: https://hackcontrol.org/cases/what-is-the-impact-of-social-engineering-attacks/ (Accessed: 10 October 2023).

*16 ransomware examples from recent attacks - CrowdStrike* (2023) *crowdstrike.com*. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-examples/ (Accessed: 10 October 2023).

Shea, S. (2023) *8 types of ransomwares: Examples of past and current attacks*, *Security*. Available at: https://www.techtarget.com/searchsecurity/feature/4-types-of-ransomware-and-a-timeline-of-attack-examples#:~:text=Zcryptor%20was%20one%20of%20the,ransom%20increased%20to%205%20bitcoin (Accessed: 10 October 2023).

Ocasio, K. (2023) *6 tech support Scams You should know about*, *Small Business Trends*. Available at: https://smallbiztrends.com/2023/08/tech-support-scams.html (Accessed: 11 October 2023).

*The Anatomy of Tech Support Scams* (no date) *Malwarebytes*. Available at: https://www.malwarebytes.com/resources/anatomy-of-tech-support-scams (Accessed: 11 October 2023).

*The Anatomy of Tech Support Scams* (no date) *Malwarebytes*. Available at: https://www.malwarebytes.com/resources/anatomy-of-tech-support-scams (Accessed: 11 October 2023).

Ritchie, J.N.& A. and Jayanti, S.F.-T., and A. (2021) *Tech Support Scams*, *Federal Trade Commission*. Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/tech-support-scams (Accessed: 11 October 2023).

(No date) *17 common job frauds and how to protect yourself | indeed.com*. Available at: https://www.indeed.com/career-advice/finding-a-job/job-scams (Accessed: 11 October 2023).

Seah, L. (2023) *Is this a fake recruiter? Six recruitment fraud Red Flags*, *Technology and Engineering Workforce Solutions: Global STEM Jobs*. Available at: https://www.airswift.com/blog/recruitment-scam-red-flags (Accessed: 11 October 2023).

Palta, R. (2023) *What are recruiting frauds? 6 ways to spot recruitment fraud*, *Flex Jobs Job Search Tips and Blog*. Available at: https://www.flexjobs.com/blog/post/know-recruitment-fraud/ (Accessed: 11 October 2023).

*What is credential harvester attack?* (2022) *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/what-is-credential-harvester-attack/ (Accessed: 11 October 2023).

(No date) *How to detect & prevent credential harvesting attacks in 2023*. Available at: https://datadome.co/learning-center/how-to-detect-prevent-credential-harvesting-attacks/ (Accessed: 11 October 2023).

*Best platforms to practice ethical hacking* (no date) *Knowledge Hut*. Available at: https://www.knowledgehut.com/blog/security/practice-ethical-hacking#websites-to-practice-ethical-hacking%C2%A0 (Accessed: 11 October 2023).

Luque, C. (no date) *Credential harvesting - how phishing attacks have evolved and how organizations can adapt to prevent new age cyber-attacks*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/credential-harvesting-how-phishing-attacks-have-evolved-chris-luque (Accessed: 11 October 2023).

Mimecast (no date) *What is credential harvesting? Mimecast*. Available at: https://www.mimecast.com/blog/what-is-credential-harvesting/ (Accessed: 11 October 2023).

*Watering hole attacks* (no date) *Malwarebytes*. Available at: https://www.malwarebytes.com/watering-hole-attack (Accessed: 11 October 2023).

Holland, W. by: M. (no date) *17 manipulation tactics abusers use*, *Choosing Therapy*. Available at: https://www.choosingtherapy.com/manipulation-tactics/ (Accessed: 11 October 2023).

Sampliner (2023) *What is elicitation: Top requirement elicitation techniques for 2023*, *Simplilearn.com*. Available at: https://www.simplilearn.com/what-is-elicitation-article#what_is_elicitation (Accessed: 11 October 2023).