

**Report**

**Social Engineering**

**Presented By**

**Mr. Itthikon Amonkhana 65102010172**

**Mr. Tarnakit Pornvoravanij 65102010555**

**Faculty of Science, Department of Data Engineering**

**Srinakharinwirot University, Bangkok, Thailand.**

**December, 2024**

**Abstract**

Social engineering is one of the most critical cybersecurity threats, which manipulates human behavior to gain access to sensitive information. Attackers exploit emotions such as fear, urgency, and curiosity in deceiving individuals into releasing personal data or compromising organizational security. Common techniques include phishing, pretexting, and deepfakes, all using technology to further deceptively manipulate. The attacks have become more personalized and difficult to detect with the increasing use of artificial intelligence in the attacks. These risks can be mitigated by creating an environment of cybersecurity awareness, using advanced detection tools, and training individuals in recognizing and preventing such threats. This report looks into the psychological factors behind social engineering attacks, common methods used, consequences, and ways to effectively address these attacks.

Table of Contents

[Introduction 1](#_Toc185012319)

[Social Engineering 2](#_Toc185012320)

[Psychological Underpinnings of Social Engineering 2](#_Toc185012321)

[Fear 2](#_Toc185012322)

[Greed 3](#_Toc185012323)

[Helpfulness 3](#_Toc185012324)

[Urgency 3](#_Toc185012325)

[Curiosity 4](#_Toc185012326)

[Summary 4](#_Toc185012327)

[Common Pattern of Social Engineering 5](#_Toc185012328)

[Attacks Classification 6](#_Toc185012329)

[Common Social Engineering Techniques and Scenarios 8](#_Toc185012330)

[Phishing and Spear Phishing 8](#_Toc185012331)

[Pretexting 8](#_Toc185012332)

[Baiting and Quid Pro Quo 8](#_Toc185012333)

[Tailgating and Physical Intrusion 9](#_Toc185012334)

[Vishing and Smishing 9](#_Toc185012335)

[Consequences of Social Engineering Attacks 10](#_Toc185012336)

[Real-World Case Studies 11](#_Toc185012337)

[1. Notable Cyber-Attacks Leveraging Social Engineering 11](#_Toc185012338)

[2. Analysis of Attack Vectors 12](#_Toc185012339)

[6 Keys To Prevent Social Engineering 13](#_Toc185012340)

[1.Check the source 13](#_Toc185012341)

[2.Knowledge is power 13](#_Toc185012342)

[3.Slow it down 13](#_Toc185012343)

[4.Privacy, Privacy, Privacy! 14](#_Toc185012344)

[5.Is this realistic? 14](#_Toc185012345)

[6.Educate 14](#_Toc185012346)

[Incident Response and Mitigation 15](#_Toc185012347)

[Containment Measures 15](#_Toc185012348)

[Forensic Analysis 15](#_Toc185012349)

[Communication and Reporting 16](#_Toc185012350)

[Future Trends in Social Engineering 17](#_Toc185012351)

[Best Practices and Recommendations 18](#_Toc185012352)

[Conclusion 20](#_Toc185012353)

[References 22](#_Toc185012354)

# Introduction

Digital communication is fast and convenient, but it is also at risk of theft or attack. Despite advanced security and encryption technologies, humans remain the weakest link in the cybersecurity chain.

Social engineering is a manipulation technique that takes advantage of human error to steal or access personal information. In cybercrime, these “human” scams often trick unsuspecting users into revealing information, spreading malware infections, or granting access to restricted systems. Attacks can occur online, in person, or through other interactions.

Digital communication is fast and convenient, but it is also at risk of theft or attack. Despite advanced security and encryption technologies, humans remain the weakest link in the cybersecurity chain.

Hackers often exploit users' lack of knowledge about cybersecurity. With rapid advancements in technology, many people are unaware of threats like malicious download requests. Some even fail to recognize the importance of protecting personal information, leaving them unsure of how to secure themselves and their data.

Raising awareness about cybersecurity threats is crucial to helping users protect themselves. Many free resources are available to educate individuals on these issues. By improving awareness and understanding, individuals, communities, and workplaces can better prepare and defend themselves against the evolving nature of cyber-attacks.

In the sections that follow, this report will further explore the tactics and motivations of social engineers, discuss common attack methods, present real-world examples, and offer practical recommendations for prevention and mitigation. By gaining a deeper understanding of these human-centered threats, individuals, organizations, and communities can better prepare themselves against the evolving landscape of social engineering attacks.

# Social Engineering

## Psychological Underpinnings of Social Engineering

Social engineering is when someone tries to influence another person’s actions, often in a way that isn’t in that person’s best interest. Instead of breaking into computers with technical skills, attackers focus on human emotions—like fear or urgency—to push people into doing things they normally wouldn’t, such as sharing personal information or giving away passwords. Getting tricked by these tactics doesn’t mean you’re not smart. Even experienced cybersecurity professionals can be fooled. In one test by the company Social-Engineer, LLC (SECOM), trained experts still ended up giving away sensitive information during a “vishing” (voice phishing) attempt.

Why are these tricks so effective, even against people who should know better? It all comes down to our emotional responses. When we’re scared or feeling pressured, our brains can switch into a “fight-or-flight” mode, often called an “amygdala hijack.” This means we rely on quick, emotional reactions instead of careful, logical thinking. Attackers know this, and they exploit these moments of panic to get us to respond without thinking.

Here ar e a few examples of how attackers use emotional pressure to influence people’s decisions.

### Fear

Fear is a strong, unpleasant feeling that we experience when we think we are in danger. Cybercriminals often take advantage of this emotion because it’s so powerful and easy to trigger. For example, imagine getting an email claiming that your bank account has been hacked and telling you to change your password right away. Even if the email is fake, you might feel so nervous that you quickly follow their instructions without stopping to think carefully.

An even scarier example is a “virtual kidnapping” scam. In this case, the criminal pretends that they have kidnapped someone you love, and they demand a ransom. Because you’re so afraid for your family member’s safety, you might pay before you realize it’s a scam. By playing on our fears, attackers push us into reacting without using logic, which helps them get what they want.

### Greed

The Cambridge dictionary defines greed as an “intense and selfish desire for something, especially wealth.” This innate characteristic of mankind is what social engineers often take advantage. One notorious case is the “419 Nigerian scam.” In this scheme the criminals pose as rich foreigners who require assistance in moving over a great deal of money. They say that after you make an initial payment or give them your banking information, they will return a large percentage of their riches in the end. Many victims, mesmerized by the notion of quick cash, consequently divulge rather delicate information blindly never knowing they have been scammed.

### Helpfulness

Most of us appreciate the virtue of being respectful and being compliant, particularly to those in authority, ever since we were young. As cybercriminals are aware of this, they deploy it against us. They frequently find their way to new recruits who are enthusiastic about accomplishing something right. In a lot of regions, kids are raised to never question their bosses’ orders. So attackers pretend to be in authority—a manager or a CEO, for example—and send emails requesting a ‘little favor’ that needs to be done quickly. This favor may include gifting card codes, sensitive financial information, or login details. Since it appears to have originated from a trusted and high-ranking individual, a lot of people do not think twice before divulging information that they would otherwise protect.

### Urgency

A lot of social engineering scams try to force you to respond instantly. Rush – this is what attackers aim for, so that you do not think too much. For instance, you might get a notice regarding an erroneous transaction on your charge card and you must rectify it instantly. When cannot check with them, suddenly there is an email from someone posing as your boss requesting something. If people are in a hurry, there is a high tendency to commit errors which will aid the attacker.

### Curiosity

Curiosity is another technique used in social engineering. The attackers promise something of interest or advantageous to deceive the victims. This type of attack could be as simple as sending an email stating “Your Amazon purchase for the amount of $800.00 is ready to ship. Click here to view your order.” This type of email or text may trigger the curiosity of the target, who may feel compelled to click on the link.

### Summary

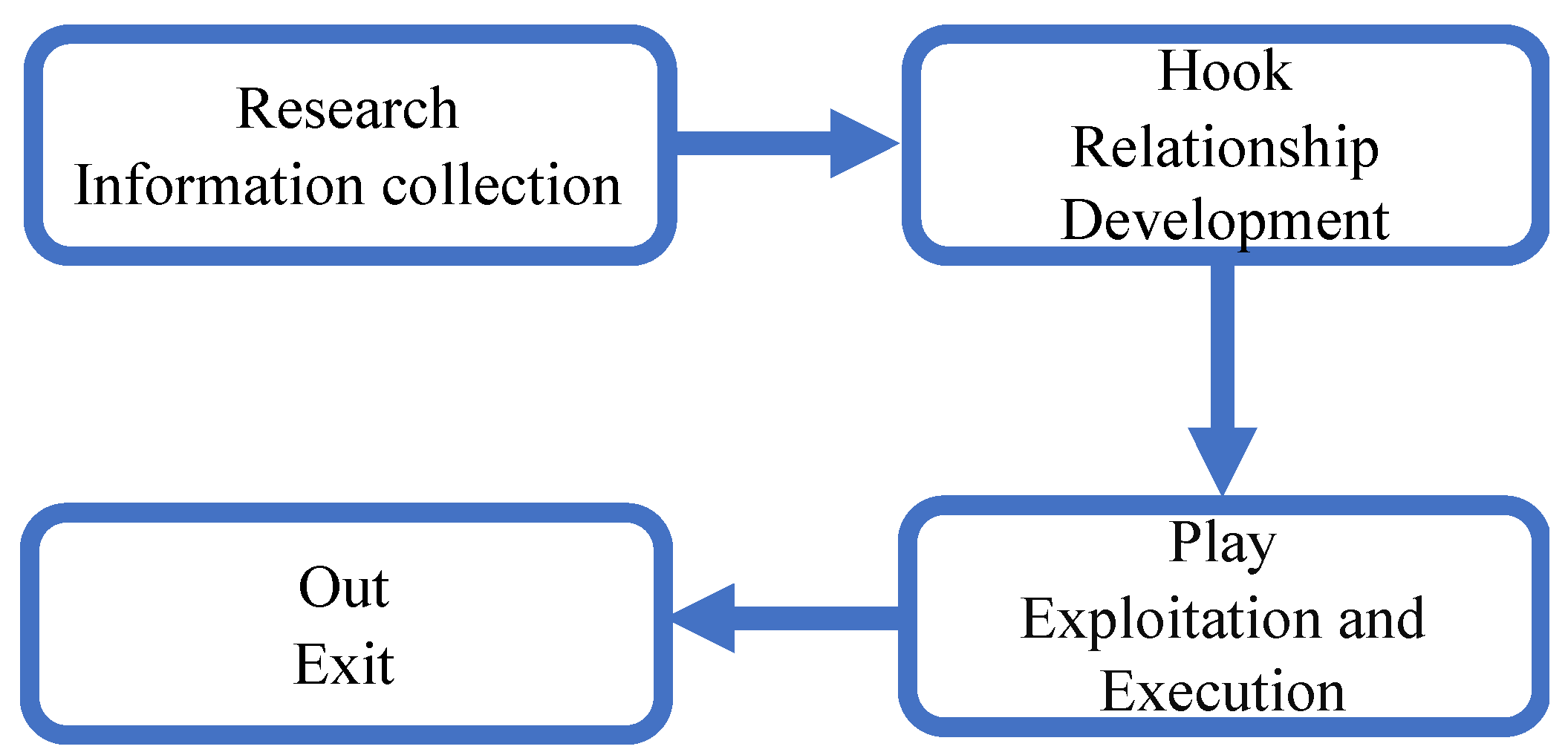
In addition to leveraging human emotions like fear, greed, helpfulness, urgency, and curiosity, social engineers skillfully apply principles of influence—such as reciprocity, commitment, social proof, authority, liking, and scarcity—to manipulate their targets. These tactics don’t operate in isolation; rather, they often work together. For example, a request from a figure of authority might also create a sense of urgency or tap into a victim’s desire to be helpful. The effectiveness of these methods can vary based on cultural, organizational, or individual factors, meaning certain approaches might resonate more powerfully in different settings.

Understanding these psychological underpinnings is the first step in building resilience against social engineering attacks. By recognizing emotional triggers and influence principles as they occur, individuals become better equipped to pause and think critically before taking action. Regular training, awareness programs, and fostering a culture of healthy skepticism can further reduce vulnerability

## Common Pattern of Social Engineering

Nowadays, social engineering attacks are some of the most dangerous cybersecurity threats. Even though they sometimes can be detected, it is really hard to stop them at all. Attackers, so-called social engineers, manage to deceive people into giving them sensitive information. Later, this information can be used to achieve certain goals or sold on the black market or the dark web. Big Data has become such that it is now utilized by the attackers to draw valuable insights from large data sets, enabling them to gather and sell huge amounts of personal and business data as if it were a common product.

Even though social engineering attacks may look different from each other, they often follow a similar pattern with four main stages. These stages are: (1) gathering information about a target, (2) building a relationship with the target, (3) making use of the collected information to carry out the attack, and (4) leaving without leaving any clues behind. Figure 1 shows these stages of a social engineering attack.

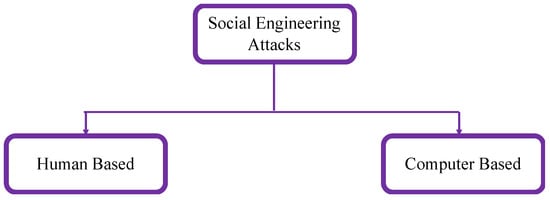


**Figure 1.** Social engineering attack stages [2].

During the research phase, sometimes called information gathering, the attacker picks a victim based on certain criteria. During the hook phase, the attacker earns the victim’s trust, usually through direct communication or emails. In the play phase, the attacker uses emotional tactics to convince the victim to reveal sensitive information or make security errors. Finally, in the out phase, the attacker leaves the scene without leaving any evidence behind.

## Attacks Classification

Social engineering attacks can be classified into two categories: human-based or computer-based as illustrated in **Figure 2**.



**Figure 2.** Social engineering attacks classification [2].

In human-based attacks, the attacker meets the victim face-to-face and talks to them directly to get the information they want. This kind of attack happens in person, so it usually only affects a small number of people.

On the other hand, software-based attacks use computers or smartphones to get information. These attacks can target many people quickly. One example of this is the Social Engineering Toolkit (SET), which is often used to send fake emails for spear phishing.

Social engineering attacks can be divided into three main types depending on how they happen: social, technical, and physical attacks, as shown in **Figure 3**.

A diagram of a social engineering

Description automatically generated

**Figure 3.** Social engineering attacks classification [2].

Social-based attacks use relationships with victims to trick them by playing with their feelings and emotions. These types of attacks are very dangerous and often successful because they involve interacting with people. Examples of social-based attacks include baiting and spear phishing.

Technical-based attacks happen online, using social networks or websites to get important information like passwords, credit card numbers, or answers to security questions.

Physical-based attacks are when attackers do something in person to gather information about the target. For example, they might look through dumpsters to find valuable documents.

## Common Social Engineering Techniques and Scenarios

### Phishing and Spear Phishing

**Phishing** involves sending fraudulent communications, typically emails, that appear to come from reputable sources to steal sensitive data like login credentials or financial information. **Spear phishing** is a more targeted form, aiming at specific individuals or organizations by personalizing the message based on gathered information.

**Example:** In July 2020, Twitter experienced a significant breach where attackers used spear phishing techniques to compromise employee credentials. This led to unauthorized access to high-profile accounts, promoting a cryptocurrency scam.

### Pretexting

**Pretexting** involves attackers creating a fabricated scenario to obtain information or access. They often impersonate authority figures or trusted entities to build credibility and manipulate victims into providing sensitive data.

**Example:** An attacker impersonates an IT support technician, contacting employees to "verify" their login credentials to resolve a supposed issue, thereby gaining unauthorized access to the company's systems.

### Baiting and Quid Pro Quo

**Baiting** lures victims with the promise of an attractive item or service, leading them to expose sensitive information or install malware. **Quid pro quo** involves offering a service in exchange for information or access.

**Example:** An attacker leaves infected USB drives labeled "Confidential" in public areas. Curious individuals pick them up and insert them into their computers, inadvertently installing malware.

### Tailgating and Physical Intrusion

**Tailgating** occurs when an unauthorized person follows an authorized individual into a restricted area without proper credentials, exploiting human courtesy.

**Example:** An attacker waits near a secure entrance and, when an employee unlocks the door, follows them inside by engaging in small talk, bypassing security protocols.

### Vishing and Smishing

**Vishing** (voice phishing) uses phone calls to trick individuals into revealing personal information, while **smishing** (SMS phishing) employs text messages for the same purpose.

**Example:** Scammers call individuals, posing as bank representatives, claiming there's an issue with their account and requesting verification of personal details. Similarly, smishing attacks send texts with links to fake websites to harvest credentials.

## Consequences of Social Engineering Attacks

**Leakage of sensitive data**: Social engineering attacks are often aimed at obtaining confidential information. If successful, this can lead to the leakage of sensitive data, such as information on customers, employees, company finances or trade secrets.

**Financial loss**: Cybercriminals can use social engineering to defraud the company of money, whether through fraud, unauthorized fund transfers or payments to fraudulent suppliers.

**Reputational damage**: Successful social engineering attacks can seriously damage a company’s reputation. Customers and business partners may lose confidence in the company if sensitive data is leaked or if it is involved in scams.

**Disruption of operations**: Some social engineering attacks aim to disrupt company operations. This can result in service disruption, loss of productivity and significant costs to restore normal operations.

**Legal liability**: Companies can be held liable for breaches of their customers’ privacy, or for the financial consequences of a successful social engineering attack. This can lead to legal action.

**Infiltration of networks and systems**: Social engineering attacks can enable cybercriminals to break into corporate networks and systems, which can lead to cyber espionage, intellectual property theft or other forms of intrusion.

**Malware propagation**: Attackers can use social engineering to induce employees to download malware, which can compromise the security of IT systems and data.

**Loss of financial or accounting data**: Social engineering attacks can target employees responsible for finance or accounting, leading to the loss of crucial financial data or fraudulent manipulation.

## Real-World Case Studies

### 1. Notable Cyber-Attacks Leveraging Social Engineering

**Case Study: 2013 Target Breach**

* **What Happened**: Attackers sent phishing emails to an HVAC vendor working with Target. Through this, they gained access to Target's network and installed malware on the retailer's point-of-sale systems.
* **Impact**: Stolen data from 40 million credit and debit cards, costing Target millions in settlements.
* **Social Engineering Element**: The attackers exploited trust in third-party vendors to infiltrate Target's system.

**Case Study: RSA Breach (2011)**

* **What Happened**: Attackers sent phishing emails with an Excel file containing malware to RSA employees. Once opened, the malware exploited vulnerabilities to gain access to RSA’s systems.
* **Impact**: Compromised RSA’s SecureID two-factor authentication system, leading to data breaches in other companies.
* **Social Engineering Element**: The email’s subject line, "2011 Recruitment Plan," piqued employee curiosity, prompting them to open the malicious file.

**Case Study: Twitter Breach (2020)**

* **What Happened**: Hackers used phone spear phishing to trick Twitter employees into providing access credentials. This allowed them to take over high-profile accounts and post cryptocurrency scams.
* **Impact**: Affected accounts included those of Elon Musk and Bill Gates, leading to a loss of trust in Twitter’s security.
* **Social Engineering Element**: Attackers manipulated employees with convincing pretexts and urgency.

### 2. Analysis of Attack Vectors

**Building Trust**: Attackers often impersonate trusted entities (e.g., IT staff, vendors) to lower suspicion.

## 6 Keys To Prevent Social Engineering

### 1.Check the source

When you get a message, always check the source to make sure the person you are talking to is really who they say they are. If an email request looks strange or unusual, double-check the email address. If it’s someone you have talked to before, compare the address with previous emails you know are real.

If you get a phone call from someone saying they work for an organization and they ask for sensitive information, don’t just trust them right away. You can search for the official phone number of the organization and call them to confirm if the request is real or not.

### 2.Knowledge is power

It is important to ask yourself if the person contacting you has the information they should know, like your full name, date of birth, or address. For example, many social engineering attacks pretend to be someone important, like a bank or government employee. However, when they ask for something, they often don’t have your information or follow the usual process, like asking security questions before making changes to your account. Learning how real bank or government workers communicate can help you spot these fake attempts.

### 3.Slow it down

Attackers using social engineering tricks often try to make you feel a sense of urgency. They may include warnings about bad things happening if you don’t do what they ask quickly. This urgency is meant to stop you from thinking carefully about their requests. That’s why it’s very important to take your time and check carefully if you receive an email with a suspicious request. Doing this can help you avoid falling for a social engineering attack.

### 4.Privacy, Privacy, Privacy!

A big part of a successful social engineering attack is good research. Attackers will search the internet to find any information about their target. They might check your social media to look for personal details that can help them create a fake character or story to trick you.

This is why it’s very important to be careful about what you share online and who can see your profiles. Make sure your social media has good privacy settings. Also, only share necessary information online. For example, if you are making an online resume, avoid including details like your email address, phone number, or date of birth. This kind of information can make it easier for attackers to use against you.

### 5.Is this realistic?

Always ask yourself if a situation or request makes sense. Attackers depend on people not thinking carefully when they get their messages.

For example:

* Would a friend or family member really ask for money or help through an email?
* Would a famous celebrity really contact you for financial support?
* How likely is it that your boss or manager would ask for gift card payments?

Taking a moment to think about whether the request is realistic can help you avoid falling for a social engineering attack.

### 6.Educate

The best way to protect yourself from social engineering attacks is to stay one step ahead of hackers. To do this, you should learn about the **common types of social engineering attacks and how attackers usually behave**. By understanding this, you can become better at spotting social engineering attempts, even if they get through your first line of defense, like your email spam filter.

## Incident Response and Mitigation

Human-based attacks are advanced and hard to detect, making it important to reduce their impact. Mitigation focuses on minimizing damage after an attack on a person or company. Cybersecurity teams must plan actions to limit losses during emergencies.

For example, building a strong security culture among employees helps handle attacks. This approach ensures victims feel less ashamed, as attackers exploit misplaced trust, not a lack of intelligence.

### Containment Measures

* **Steps to Isolate Compromised Systems**:
  1. **Identify the Breach Scope**: Determine which accounts, systems, or networks have been compromised.
  2. **Disconnect Affected Systems**: Remove infected devices from the network to prevent lateral movement of the threat.
  3. **Revoke Access**: Reset credentials and disable accounts that have been breached.
  4. **Apply Temporary Safeguards**: Use temporary firewalls or network segmentation to contain the breach.
* **Example**: During the 2013 Target breach, containment involved isolating point-of-sale systems and temporarily restricting vendor access to prevent further infiltration.

### Forensic Analysis

* **Key Steps**:
  1. **Data Collection**: Gather logs, emails, and other evidence from the affected systems.
  2. **Analyze Attack Patterns**: Identify the tools, techniques, and processes used by the attackers.
  3. **Understand Entry Points**: Investigate how attackers gained initial access, such as through phishing emails or compromised accounts.
  4. **Document Findings**: Create a detailed report to guide future prevention strategies.
* **Example**: After the RSA breach in 2011, forensic analysis revealed that phishing emails with malicious Excel files were the attack vector.

### Communication and Reporting

* **Importance**:
  1. **Transparency**: Inform stakeholders, regulators, and clients about the breach promptly.
  2. **Minimize Misinformation**: Provide accurate details to prevent panic and maintain trust.
  3. **Regulatory Compliance**: Adhere to data breach notification laws and industry standards.
* **Example**: During the Twitter breach in 2020, the company released timely updates to the public and collaborated with law enforcement for further investigation.

## Future Trends in Social Engineering

**Deepfakes** are videos or audio recordings made with artificial intelligence to imitate people or situations in a very realistic way. Cybercriminals use deepfakes to create fake recordings of company executives or colleagues to trick employees into doing harmful things, like transferring money or sharing sensitive information. To stop deepfake threats, it’s important to have strong verification methods to check if the media is real and to make employees aware of the risks of fake multimedia content.

**Artificial Intelligence-based attacks:** Cybercriminals use AI as a powerful tool to automate and personalize their attacks. AI-based attacks can create realistic phishing emails targeting specific people or organizations by using information from social media and other sources. Detecting these attacks needs advanced security systems that can identify AI-based attack patterns and block threats before they reach users.

## Best Practices and Recommendations

**Cultural Shift in Organizations**

* **Emphasis**:
  1. Foster a culture of skepticism where employees are trained to question unsolicited communications.
  2. Encourage proactive defense mechanisms, such as reporting suspicious activities immediately.
  3. Develop an organization-wide mindset where cybersecurity is seen as everyone’s responsibility, not just the IT department’s.
* **Example**: Organizations like IBM have adopted a "security-first culture" where employees undergo regular phishing simulations to identify gaps in awareness.

**Continuous Learning and Security Literacy**

* **Key Points**:
  1. Implement regular training programs on identifying social engineering attacks like phishing or smishing.
  2. Stay updated on the latest cybersecurity trends and threats, leveraging online resources or partnerships with cybersecurity firms.
  3. Use gamified learning tools to engage employees in security practices.
* **Example**: The SANS Institute provides training programs tailored to educate employees about current cybersecurity threats.

**Collaboration and Information Sharing**

* **Importance**:
  1. Share threat intelligence between organizations to build collective knowledge and resilience against attacks.
  2. Partner with law enforcement to identify and address major security threats.
  3. Join industry-specific Information Sharing and Analysis Centers (ISACs) to receive real-time updates about potential vulnerabilities.
* **Example**: The Financial Services ISAC (FS-ISAC) helps financial institutions share threat intelligence and mitigate risks collectively.

# Conclusion

Social engineering has emerged as one of the most widespread and hazardous threats in the field of cybersecurity, which exploits human behavior and psychological vulnerabilities to get past traditional security measures. Techniques such as phishing, spear phishing, pretexting, baiting, vishing, and deepfakes show the creativity and deception attackers use to manipulate individuals and organizations. They essentially make their targets reveal secret information, transfer money, or commit certain actions that undermine their security through various tactics that manipulate emotional feelings, such as fear, urgency, greed, and curiosity. In this regard, attackers take advantage of artificial intelligence capabilities that not only make attacks more sophisticated but also increase their potential to create more credible scenarios and personalized messages.

The consequences are serious and many-sided, including leakage of sensitive data, financial losses, reputational damage, operational disruption, and even legal liability. Many social engineering attacks target individuals and organizations, taking advantage of the gap in awareness, trust, and security protocols. Real-life case studies, such as the Target and Twitter breaches, demonstrate how devastating social engineering can be and underline the need for robust defenses.

These threats, therefore, call for both proactive and reactive measures in order to engage them effectively. At an individual level, users need to be able to question the legitimacy of requests, source check properly, and view unsolicited communications with skepticism. Setting privacy high on social networks and disclosing only minimal information about personal life can limit the amount of data available to the attacker. While this is in place, organizations have to inculcate a security-first culture that promotes awareness programs, employee training, and attack simulations to test preparedness. Incident response planning for resilience, such as forensic analysis and containment, becomes very important in building up post-attack damage limitation.

The more advanced mitigation techniques involve deploying AI-powered detection systems, anomaly detection methods such as DAS, and multi-factor authentication to reduce vulnerabilities. In addition, organizations must put greater focus on collaboration and information sharing, ensuring that employees from top to bottom understand cybersecurity as a shared responsibility.

Social engineering attacks underpin the call for holistic cybersecurity awareness, technology, and culture. By tackling the human aspect as a central vulnerability, organizations and individuals will better defend themselves against these shifting threats. It is through focusing on continuous learning, making the most of new tools, and instilling a skeptical yet informed mentality that data, systems, and confidence can be protected from social engineering. We can be prepared for the constantly changing landscape of cybersecurity challenges through such efforts.

# References

[1] Social-Engineer, "The Psychology Behind Social Engineering," [Online]. Available: <https://www.social-engineer.com/the-psychology-behind-social-engineering/>. [Accessed: 13-Dec-2024].

[2] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," Future Internet, vol. 11, no. 4, p. 89, Apr. 2019. [Online]. Available: <https://doi.org/10.3390/fi11040089>. [Accessed: 13-Dec-2024].

[3] Altospam, " Social engineering, an invisible threat: trends and developments," [Online]. Available: <https://www.altospam.com/en/news/social-engineering-an-invisible-threat-trends-and-developments/>. [Accessed: 13-Dec-2024].

[4] PhishProtection, "Phishing Case Studies: Learning from the Mistakes of Others," [Online]. Available: <https://www.phishprotection.com/phishing/phishing-case-studies-learning-from-the-mistakes-of-others>. [Accessed: 13-Dec-2024].

[5] Fortinet, "Pretexting," [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/pretexting>. [Accessed: 13-Dec-2024].

[6] SysadminSage, "Examples of Social Engineering," [Online]. Available: <https://sysadminsage.com/examples-of-social-engineering/>. [Accessed: 13-Dec-2024].

[7] Expert Insights, "Phishing, Vishing, Smishing, Whaling, and Pharming: How to Stop Social Engineering Attacks," [Online]. Available: <https://expertinsights.com/insights/phishing-vishing-smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/>. [Accessed: 13-Dec-2024].

[8] B. Krebs, "Target Hackers Broke in Via HVAC Company," Krebs on Security, Feb. 2014. [Online]. Available: <https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/>. [Accessed: 13-Dec-2024].

[9] BBC News, "Twitter hack: What went wrong and why it matters," Jul. 2020. [Online]. Available: <https://www.bbc.com/news/technology-53607374>. [Accessed: 13-Dec-2024].

[10] Fortinet, "Social Engineering," [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/social-engineering>. [Accessed: 13-Dec-2024].

[11] StickmanCyber, "6 Ways to Prevent Social Engineering Attacks," [Online]. Available: <https://www.stickmancyber.com/cybersecurity-blog/6-ways-to-prevent-social-engineering-attacks>. [Accessed: 13-Dec-2024].

[12] D. Goodin, "RSA hack hit US defense secrets," The Register, Apr. 2011. [Online]. Available: <https://www.theregister.com/2011/04/04/rsa_hack_howdunnit/>. [Accessed: 13-Dec-2024].

[13] IBM, "IBM Blog," [Online]. Available: <https://www.ibm.com/blog/>. [Accessed: 13-Dec-2024].

[14] SANS Institute, "Cyber Security Courses," [Online]. Available: <https://www.sans.org/cyber-security-courses/>. [Accessed: 13-Dec-2024].

[15] FS-ISAC, "Financial Services Information Sharing and Analysis Center," [Online]. Available: <https://www.fsisac.com/>. [Accessed: 13-Dec-2024].