

Lab - Social Engineering

# Objectives

Research and identify social engineering attacks

# Background / Scenario

Social engineering is an attack with the goal of getting a victim to enter personal or sensitive information, this type of attack can be performed by an attacker utilizing a keylogger, phishing email, or an in-person method. This lab requires the research of social engineering and the identification of ways to recognize and prevent it.

# Required Resources

* PC or mobile device with internet access

# Instructions

Using a web browser f ind the article “Methods for Understanding and Reducing Social Engineering Attacks” on the SANS Institute website. A search engine should easily f ind the article.

The SANS Institute is a cooperative research and education organization that offers information security training and security certification. The SANS Reading Room has many articles that are relevant to the practice of cybersecurity analysis. You can join the SANS community by creating a f ree user account in order to access to the latest articles, or you can access the older articles without a user account.

Read the article or choose another article on social engineering, read it, and answer the following questions:

1. What are the three methods used in social engineering to gain access to information?

* **ELECTRONIC ACCESS**: The attacker makes use of these three attacks in order to gain sensitive information or access to systems:
* **1. Phishing:**
* Phishing is a broad technique used in social engineering where attackers send fraudulent messages (often via email, text, or websites) that appear to come from a legitimate source, like a trusted institution (e.g., a bank or social media platform). The goal is to trick individuals into providing sensitive information like passwords, credit card numbers, or personal details. Phishing campaigns are typically sent to large numbers of people, hoping that a few will fall for the scam.
* **Example**: A user receives an email that looks like it's from their bank, asking them to click a link to verify their account. The link takes them to a fake website that looks like the bank’s site, where they input their login credentials, which are then stolen by the attacker.
* **2. Spear Phishing:**
* Spear phishing is a more targeted version of phishing. Instead of casting a wide net, attackers focus on specific individuals or organizations. The attacker personalizes the message using information about the target, such as their name, job role, or specific details about the organization, to make the scam more convincing. Since it’s more customized, spear phishing is often more effective than generic phishing.
* **Example**: A CEO receives an email that looks like it’s from a known colleague, asking them to review an important document. The email is tailored with details from the colleague’s life or work, making it seem legitimate. When the CEO clicks the link, malware is installed on their device or credentials are stolen.
* **3. Baiting:**
* Baiting involves enticing a victim with the promise of something desirable (such as free software, music downloads, or physical items like USB drives) to lure them into performing an action that compromises their security. This technique often involves the attacker leaving physical media or online downloads that seem harmless but contain malware.
* **Example**: A USB drive labeled "Confidential: 2024 Employee Salaries" is left in a public place like a parking lot. A curious employee finds it, plugs it into their work computer, and unknowingly installs malware that grants the attacker access to the organization's network.
* **PHYSICAL ACCESS**: The attacker makes physical contact with the target and makes use of these three attacks in order to gain sensitive information:
* **1. Pretexting:**
* Pretexting involves an attacker creating a fictitious scenario or "pretext" to deceive the victim into sharing sensitive information or performing an action. The attacker typically poses as someone the victim trusts, such as a coworker, a bank official, or a government representative. Pretexting relies on building a credible story to manipulate the victim into giving up private data like passwords, social security numbers, or access credentials.
* **Example**: An attacker calls an employee pretending to be from the IT department, claiming they need the employee's login credentials to resolve a technical issue. The victim, believing the request is legitimate, provides the requested information, which the attacker then uses to gain unauthorized access to the company's systems.
* **2. Tailgating (or Piggybacking):**
* Tailgating, also known as piggybacking, occurs when an unauthorized person physically follows an authorized individual into a restricted area, such as a secure building or office. This often happens when the authorized person holds a door open for someone they believe to be legitimate, either out of politeness or assumption. Tailgating exploits human trust and social norms rather than technical vulnerabilities.
* **Example**: An attacker waits outside a secure building and follows an employee who uses their access card to open the door. The attacker walks in behind the employee, acting as if they are also authorized to enter. Once inside, the attacker may access confidential information or steal physical assets.
* **3. Quid Pro Quo:**
* Quid pro quo attacks involve an exchange in which the attacker promises something of value or assistance in return for information or access. The attacker pretends to offer help (such as technical support) or benefits in exchange for sensitive information. It’s similar to baiting, but quid pro quo explicitly involves an agreement or transaction.
* **Example**: An attacker calls random employees at a company, claiming to be from technical support, offering to fix an issue in exchange for login credentials. The attacker might say, "I'm with IT and noticed you're having issues with your system; if you provide your login, I can help resolve it right now." The employee, believing they will receive assistance, shares the credentials, which the attacker uses to gain unauthorized access.

**SOCIAL MEDIA:** The attackers make use of social media to gain sensitive information and proceed to use said information either to use it against the user or create a fake profile to carry out malicious actions on the internet. Attackers might be able to gain these information by commenting sites on a profile tricking users to click a URL that promises to give something for free or those games on facebook that asks for your name could surprisingly still be used against you since attackers can use these kinds of platform in order to collect your name address and phone number and then proceed to use it to create an account and use it for their own greedy means.

1. What are three examples of social engineering attacks f rom the f irst two methods in step 2a?

### **CEO FRAUD**

CEO fraud refers to the impersonation of a CEO or another senior executive in a fake email targeted towards the employees with the power to make a transfer. It can play on the idea of authority and hierarchy – the idea that employees are desperate to impress.

CEO fraud usually targets **mid-management or senior members of staff**, as they are more likely to have the authority to approve payments or share personal information. Both of these factors contribute to the threat, making CEO’s 9 times more likely to be targeted than any other member of the organization.

**A real-life example**: the Xoom fraud

Unfortunately, this type of spear phishing campaign happens quite often. A spear-phishing attack via CEO fraud happened at Xoom in 2014. The company admitted that its financial reports in the first quarter of 2015 would highlight a one-off charge as a consequence, resulting in losses of over $30 million.

It happened because fraudsters impersonated an undisclosed senior employee requesting a transfer, and the accounts department made this transfer. The CFO (who was newly appointed to the position) immediately resigned.

**INVOICE FRAUD**

Invoice fraud is another phishing scam and is the result of criminals impersonating a known supplier to change banking information and credentials.

Typically, the fraudsters hack into your system and intercept a real invoice but change the bank details. Or they could spoof the merchant’s email address and begin a whole new thread. But in the case of Levitas Capital, the attackers relied on weak cybersecurity defenses.

**A real-life example**: the Facebook and Google fraud

Even the giants can be targeted by spear phishing attempts, and without the right controls in place, they can fall victim to cyber-criminals.

Facebook and Google had a mutual supplier, Quantas Computer Inc, based in Thailand. Between 2013 and 2015, a Lithuanian scam artist spoofed the email of this supplier and sent false invoices to both companies. This led to [losses of $23 million for Google](https://www.zdnet.com/article/lithuanian-man-pleads-guilty-to-scamming-google-and-facebook-out-of-123-million/), and over $100 million for Facebook.

Although he was later convicted, the money was never returned to either of the tech giants.

**BANK TRANSFER FRAUD**

[Bank transfer fraud](https://trustpair.com/blog/bank-transfer-fraud/) happens when criminals hack into a company’s system and send themselves funds. Wire transfer fraud grows by 13% every year, and spear phishing techniques only make that number likely to further grow.

In some cases, the fraudsters’ target is sensitive company information that will allow them to gain access to your bank account and make a transfer, undetected. So it’s important to consider how your company protects its data to prevent it from being compromised, and keeps the finances safe.

1. Why is social networking a social engineering threat?

**1. Overexposure of Personal Information:**

People often share detailed information about their lives, including their jobs, relationships, hobbies, locations, and even daily routines. This data can be leveraged by social engineers to craft convincing scams, like **phishing** or **pretexting**. Attackers can impersonate colleagues, friends, or even official entities using the information gleaned from social profiles, making their scams appear more credible.

* **Example**: A hacker finds out from your social media profile that you recently joined a new company. They send you a spear-phishing email pretending to be from your HR department, asking for sensitive data like your employee ID or bank details.

**2. Trust Exploitation:**

On social networks, people often form connections with individuals they don’t know well or at all, based on shared interests, mutual friends, or professional relationships. Attackers exploit this trust by posing as someone within the victim’s network (e.g., a friend or coworker) to gain access to more information or to manipulate the victim into sharing sensitive data.

* **Example**: An attacker sends a friend request posing as a mutual connection or creates a fake profile that looks like someone you know. Once accepted, they can message you, pretending to be your friend, and ask for personal details like your home address, phone number, or other valuable information.

**3. Social Engineering at Scale:**

Social networks allow attackers to conduct large-scale social engineering attacks efficiently. With tools that automate data collection from profiles, attackers can target many individuals or organizations at once, making it easier to craft phishing campaigns or gather intelligence on targets for future attacks.

* **Example**: An attacker scrapes data from LinkedIn to identify employees at a specific company. Using this information, they send tailored phishing emails to several employees, claiming to be from the company’s IT department, to steal login credentials.

**4. Impersonation and Fake Profiles:**

Social networks are rife with fake accounts, where attackers impersonate others to gain trust or manipulate individuals. Attackers can create profiles that mimic friends, colleagues, or well-known figures, making it easy to deceive victims into sharing private information or clicking malicious links.

* **Example**: An attacker creates a fake profile pretending to be the CEO of a company and sends connection requests to employees. Once connected, they message employees asking for confidential company data or financial transactions under the guise of authority.

**5. Information Gathering for Future Attacks:**

Attackers can gather detailed information on their targets by monitoring their social networking activity, such as status updates, photos, and connections. This information can be used in future **spear-phishing** or **pretexting** attacks, making them much more convincing and difficult to detect.

* **Example**: An attacker monitors an executive’s travel plans shared on social media. They later send an email pretending to be the executive, asking their assistant to wire money urgently while they are "out of the office on a business trip."

**Lab - Social Engineering**

1. How can an organization defend itself from social engineering attacks?

The solution is to create an in-house, custom built security awareness and

training program. It must take into consideration all the factors that affect the organization as well as the behavioral and personality factors, it must be planned, designed, implemented and measured. It must be “baked-in” to the everyday processes of the organization until it becomes part of the culture of the organization.

* Firstly, the training must be planned, there should be actual goals as to what the employees can understand and do once they have reached a certain part of the training, Then plan time to research and select the best personality test for the organization Finally the format and delivery method of the training should be determined. This should consider all factors such as training facilities available, training materials, location of employees if the organization is global, various languages. A project plan should be laid out to determine all relevant tasks, planned start and end dates for each task, predecessors and projected complete date of the training.
* Secondly, perform the personality testing once the test is completed then categorize the employees based on their personality types.
* Third, this happens once the testing and analysis is complete then the design for each category will then begin to teach them what they need to learn.
* Fourth, is to develop the security awareness training, the design should be tailored to focus on the potential strengths, andmore importantly, the weaknesses of each personality type. From the planning process,training materials must be created, facilities must be secured and schedules must be finalized.A testing of the materials should be performed on a small cross-functional group ofemployees and feedback should be collected and incorporated where appropriate. Also, this iswhere success criteria should be determined so that when results are measured, managementwill know whether or not the program is a success.
* Lastly, is to implement the security awareness training

1. What is the SANS Institute, which authored this article?

The SANS (SysAdmin, Audit, Network, Security) Institute is one of the most respected and trusted organizations in the field of information security training, research, and certification. Founded in 1989, SANS provides high-quality training and resources to cybersecurity professionals and organizations around the world.

These are some of their key aspects:

**1. Cybersecurity Training and Certification:**

SANS is best known for its **training programs** in various areas of cybersecurity, including network security, ethical hacking, digital forensics, incident response, and security management. Their training courses are highly regarded and designed for professionals at all levels, from beginners to experienced practitioners. Some of the certifications they offer are associated with the **GIAC (Global Information Assurance Certification)**, which is also maintained by SANS.

* **GIAC Certifications**: These are technical certifications that validate the skills and knowledge of cybersecurity professionals in specific domains such as penetration testing, digital forensics, and defensive security.

**2. SANS Security Resources and Research:**

The institute produces a wealth of **research papers, white papers, and security guides**. They conduct studies on emerging cybersecurity threats, vulnerability analysis, and best practices. SANS also offers free resources such as **webcasts, newsletters, and blogs** to keep professionals updated on the latest security trends and incidents.

* **SANS Reading Room**: A repository of research papers and articles written by professionals in the field, covering a wide range of cybersecurity topics.

**3. SANS Security Awareness Programs:**

SANS provides **security awareness training** for organizations to help employees understand and identify cybersecurity threats like phishing, social engineering, and ransomware. The goal of these programs is to create a strong human firewall within organizations by educating staff on security best practices.

* **SANS Securing the Human**: This is a security awareness program designed to train non-technical users on how to stay safe online and avoid falling victim to attacks.

**4. Conferences and Summits:**

SANS hosts regular **conferences and summits**, including events like **SANS Cyber Defense Initiative**, **SANS Pen Test HackFest**, and **SANS DFIR Summit** (focused on digital forensics and incident response). These gatherings bring together cybersecurity professionals to share knowledge, strategies, and tools for defending against the latest threats.

**5. Internet Storm Center (ISC):**

SANS operates the **Internet Storm Center**, a global internet monitoring and analysis system that tracks cyber threats, trends, and vulnerabilities. ISC provides a daily update of security incidents and issues that affect systems worldwide.

Overall, the SANS Institute plays a crucial role in improving cybersecurity through its comprehensive education, certifications, research, and industry leadership, helping individuals and organizations stay ahead of cyber threats.