

**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**

Table of Contents

[Introduction 1](#_Toc184993738)

[Social Engineering: Understanding the Human Factor in Modern Cybersecurity 1](#_Toc184993739)

[Social Engineering 3](#_Toc184993740)

[Psychological Underpinnings of Social Engineering 3](#_Toc184993741)

[Fear 3](#_Toc184993742)

[Greed 4](#_Toc184993743)

[Helpfulness 4](#_Toc184993744)

[Urgency 5](#_Toc184993745)

[Curiosity 5](#_Toc184993746)

[Summary 5](#_Toc184993747)

# Introduction

## Social Engineering: Understanding the Human Factor in Modern Cybersecurity

Today, everyone can communicate digitally, and exchange information quickly, making it very convenient. However, exchanging information digitally is at risk of being stolen or attacked. Advanced security technologies and sophisticated encryption methods have become standard practices for communication. However, humans remain a major weakness 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.

Social engineering scams have got their origin from action and thought processes of human beings therefore, social engineering attacks can effectively steer user behavior. Users will have their intent, an understanding of what drives users into taking action gives an opportunity to the attackers to trick and control the users.

Most likely, hackers will also exploit the lack of certain users' knowledge. Due to the rapid improvement of technology, many consumers and employees do not know some threats such as aggressive download requests. Others do not recognize a fair fraction of their personal information (like their own phone numbers) understanding, thus leaving many users directionless in how to secure themselves as well as their data.

The one difficult disseminated say the new culture, and that do assist users secure the target is scanning awareness while a number of free resources targeting similar problems are available. This clearly demonstrates that if user is able to comprehend the situation then all users the communities and the workplaces can get ready, cope and secure themselves against the ever-changing dimension of the 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