

Phishing Assessment

Module 2.2: Social Engineering vs. Phishing

Table of Contents


1. Social Engineering
2. Difference between Social Engineering & Phishing

1. Social Engineering

PAST

Social Engineering

Module 2.2
Social Engineering vs.
Phishing



Psychological manipulation of people to take actions or reveal sensitive information.

Unlike cyberattacks targeting software or hardware flaws, it exploits human behavior, trust, and emotions to achieve its goals.

Page 3 of 7

Social engineering is a broad term that refers to the psychological manipulation of people to perform actions or divulge confidential information. Unlike cyberattacks that exploit software or hardware vulnerabilities, social engineering preys on human behavior, trust, and emotion to achieve its objectives.

Goals of Social Engineering:

- To gain unauthorized access to sensitive information (e.g., passwords, account details, security credentials).
- To influence someone to take action that benefits the attacker, such as executing a payment or downloading malware.
- To exploit human psychology, such as trust, fear, greed, or helpfulness, to bypass security measures.

How It Works: Attackers use various tactics to manipulate individuals into breaking standard security practices or revealing sensitive information. Social engineering can occur in person, over the phone, via email, or through other digital channels. The attacker typically establishes trust or creates a sense of urgency, tricking the victim into following through on a request they might otherwise question.

PAST

Social Engineering

Module 2.2
Social Engineering vs. Phishing


Where can someone socially engineer you?



In-Person



Phone Call



Email



Text Messages



Social Media

Page 4 of 7

Where can someone socially engineer you?

In-Person Scenarios: Attackers may pose as colleagues, repair technicians, or officials to gain access to restricted areas, extract information through casual conversation, or create a sense of urgency to manipulate decisions.

Phone Call: Pretending to be a customer support agent, a company representative, or even a friend to extract information.

Email: Sending deceptive emails that appear legitimate to trick recipients into sharing sensitive information or clicking malicious links.

Text Messages: Impersonating trusted entities in apps like WhatsApp, Slack, or Discord to extract information.

Social Media: Creating fake profiles or sending direct messages to gather information or manipulate targets.

Types of Social Engineering:



Pretexting

The attacker fabricates a believable story (pretext) to obtain sensitive information.

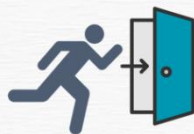
Pretexting: The attacker fabricates a believable story (pretext) to obtain sensitive information. For example, the attacker might pretend to be an IT professional asking for login credentials to "resolve a technical issue."



Baiting

Offering something tempting in exchange for login credentials or access to systems.

Baiting: Offering something tempting (such as free software or access to exclusive content) in exchange for login credentials or access to systems.



Tailgating

Physically following someone into a secure area by pretending to be someone authorized or leveraging social cues to avoid questioning.

Tailgating: Physically following someone into a secure area by pretending to be someone authorized or leveraging social cues to avoid questioning.



Impersonation

Attackers often impersonate authority figures, colleagues, or trusted contacts to trick the victim into acting quickly or divulging information.

Impersonation: Attackers often impersonate authority figures, colleagues, or trusted contacts to trick the victim into acting quickly or divulging information.



Dumpster Diving

Searching through trash for sensitive information.

Dumpster Diving: Searching through trash for sensitive information. For Examples: Finding discarded documents containing passwords, account details, or confidential plans. OR retrieving old electronics that may have unencrypted data.

2. Difference between Social Engineering & Phishing

PAST

Difference between Social Engineering & Phishing

Module 2.2
Social Engineering vs. Phishing

Social Engineering	Phishing
<ul style="list-style-type: none"> Manipulating people to reveal information or perform actions using psychological tactics. Broad – includes both digital and in-person tactics. Can involve face-to-face interactions or online deception. 	<ul style="list-style-type: none"> A specific type of social engineering using deceptive digital communication. Narrow – focuses on digital communication. Entirely digital (email, websites, texts).

Page 6 of 7

What is the real difference between Social Engineering & Phishing?

Social Engineering is like an umbrella term that includes phishing as one of its techniques. Phishing is a subset of social engineering.

Phishing is one of the types in social engineering, however not all social engineering attacks are phishing. Social engineering is a broad concept that includes both digital and in-person tactics. It can happen over the phone, in face-to-face interactions, or through online deception. Phishing, on the other hand, is a specific form of social engineering that occurs exclusively in digital environments, using emails, text messages, or fake websites to steal information. Simply put, all phishing attacks are social engineering, but not all social engineering attacks are phishing.

Summary

Social engineering is a broad category that includes digital and in-person tactics, such as impersonation, tailgating, and baiting. Phishing is a specific type of social engineering that occurs exclusively in digital format, primarily through emails, text messages, or fake websites designed to steal sensitive information. In essence, phishing is a subset of social engineering that focuses on deceptive online communication.

- END -