2.3.4 Social Engineering Motivation Facts

There are many social engineering attacks, types of attackers, and motivation techniques.

This lesson covers the following topics:

- Social engineering attacks
- Types of attackers
- Types of motivation techniques

Social Engineering Attacks

The following table describes a few social engineering attacks.

Attack	Description
Shoulder surfing	Shoulder surfing involves looking over someone's shoulder while that person works on a computer or reviews documents. This attack's purpose is to obtain usernames, passwords, account numbers, or other sensitive information.
Eavesdropping	Eavesdropping is an unauthorized person listening to private conversations between employees or other authorized personnel when sensitive topics are being discussed.
USB and keyloggers	When on site, a social engineer also has the ability to steal data through a USB flash drive or a keystroke logger. Social engineers often employ keystroke loggers to capture usernames and passwords. As the target logs in, the username and password are saved. Later, the attacker uses the username and password to conduct an exploit.
Spam and spim	When using spam, the attacker sends an email or banner ad embedded with a compromised URL that entices a user to click it. Spim is similar, but the malicious link is sent to the target using instant messaging instead of email.
Hoax	Email hoaxes are often easy to spot because of the bad spelling and terrible grammar. However, hoax emails use a variety of tactics to convince the target they're real.

Types of Attackers

The following table describes different types of attackers.

Type	Description
Insider	An insider could be a customer, a janitor, or even a security guard; but most of the time, it's an employee. Employees pose one of the biggest threats to any organization. There are many reasons why an employee might become a threat. The employee could: ▪ Be motivated by a personal vendetta because they are disgruntled. ▪ Want to make money. ▪ Be bribed into stealing information. Sometimes, an employee can become a threat actor without even realizing it. This is known as an unintentional threat actor. The employee may create security breaches doing what seems to be harmless day-to-day work. An unintentional threat actor is the most common insider threat.

Hacker	Generally speaking, a hacker is any threat actor who uses technical knowledge to bypass security, exploit a vulnerability, and gain access to protected information. Types of hackers include: ▪ Those motivated by bragging rights, attention, and the thrill. ▪ Hacktivists with a political motive. ▪ Script kiddies, who use applications or scripts written by much more talented individuals. ▪ A white hat hacker, who tries to help a company see the vulnerabilities that exist in its security. ▪ Cybercriminals, who are motivated by significant financial gain. They typically take more risks and use extreme tactics. Corporate spies are a sub-category of cybercriminal.
Nation state	Attacks from nation states have several key components that make them especially powerful. Typically, nation state attacks: ▪ Are highly targeted. ▪ Identify a target and wage an all-out war. ▪ Are extremely motivated. ▪ Use the most sophisticated attack techniques of all the attackers. This often includes developing completely new applications and viruses in order to carry out an attack. ▪ Are well financed.

Types of Motivation Techniques

The following table describes types of techniques a social engineer uses to motivate an employee to provide information.

Technique	Description
Authority and fear	Authority techniques rely on power to get a target to comply without questioning the attacker. The attacker pretends to be a superior with enough power that the target will comply right away without question. The attacker could also pretend to be there in the name of or upon the request of a superior. Authority is often combined with fear. If an authority figure threatens a target with being fired or demoted, the target is more likely to comply without a second thought.
Social proof	With a social proof technique, the attacker uses social pressure to convince the target that it's okay to share or do something. In this case, the attacker might say, "If everybody is doing it, then it's okay for you to do it, too."
Scarcity	Scarcity appeals to the target's greed. If something is in short supply and will not be available, the target is more likely to fall for it.
Likeability	Likeability works well because humans tend to do more to please a person they like as opposed to a person they don't like.
Urgency	To create a sense of urgency, an attacker fabricates a scenario of distress to convince an individual that action is immediately necessary.
Common ground and shared interest	Common ground and shared interest work because sharing a hobby, life experience, or problem instantly builds a connection and starts forming trust between two parties.