Common attacks and their effectiveness

Previously, you learned about past and present attacks that helped shape the cybersecurity industry. These included the LoveLetter attack, also called the ILOVEYOU virus, and the Morris worm. One outcome was the establishment of response teams, which are now commonly referred to as computer security incident response teams (CSIRTs). In this reading, you will learn more about common methods of attack. Becoming familiar with different attack methods, *and* the evolving tactics and techniques threat actors use, will help you better protect organizations and people.
Phishing

Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.
Some of the most common types of phishing attacks today include:
- **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
- **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
- **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
- **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
- **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

Malware
Malware is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.
Some of the most common types of malware attacks today include:
- **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
- **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
- **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
- **Spyware:** Malware that's used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

Social Engineering
Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It's the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:
- **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
- **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.
- **USB baiting:** A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
- **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

Social engineering principles

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it's also a risk.

Reasons why social engineering attacks are effective include:
- **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
- **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they're told.
- **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others' trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
- **Scarcity:** A tactic used to imply that goods or services are in limited supply.
- **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.
- **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.
- **Urgency:** A threat actor persuades others to respond quickly and without questioning.

Key takeaways

In this reading, you learned about some common attacks and their impacts. You also learned about social engineering and why it's so successful. While this is only a brief introduction to attack types, you will have many opportunities throughout the program to further develop your understanding of how to identify and defend against cybersecurity attacks.