

CompTIA Security+

Lecture 05

SY0-701

Social Engineering

By
Dr. Khaled ELMenshawy

Lecture

05

LEARNING OUTCOMES

- Understanding the meaning of Social Engineering.
- Recognize the types of Motivational Triggers.
- Understanding Impersonation.
- Recognize different types of Impersonation.
- Understanding phishing attacks.
- Recognize the types of phishing attacks.
- Understanding Malware.
- Recognize different types of malware
- Recognize the indications of malware attacks.

What is Social Engineering?

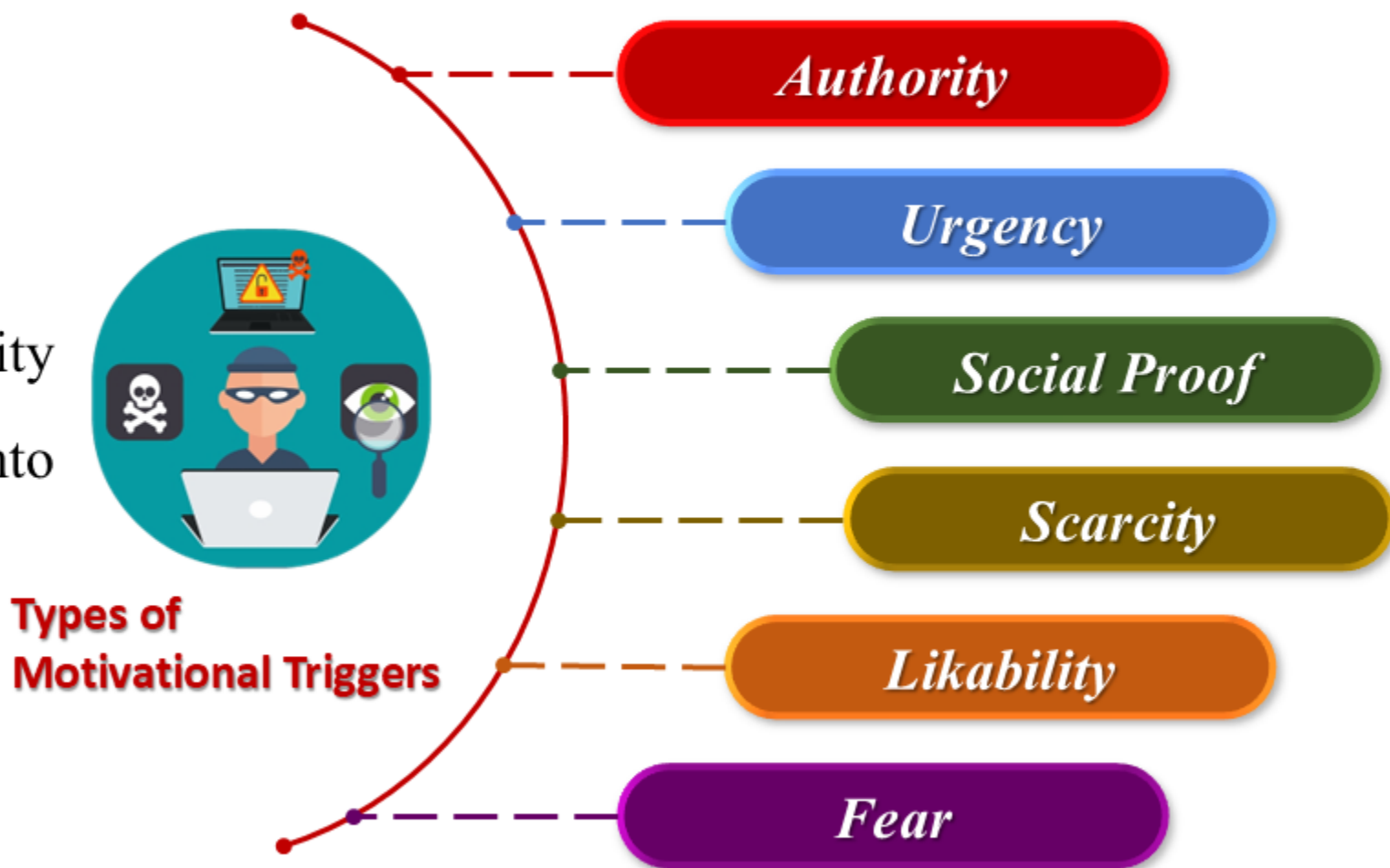
Social Engineering; is the *tactic of manipulating, influencing, or deceiving* a victim in order to *gain control over a computer system*, or to steal personal and financial information.

Steps for the social engineering attack cycle are usually as follows:

- **Prepare;** by gathering background information about the victim.
- **Infiltrate;** by establishing a relationship or initiating an interaction, started by *building trust*.
- **Exploit;** the attacker uses both information and relationships to exploit the victim without raising suspicion.
- **Disengage;** by closing the interaction and removing all traces (covering tracks).

What is motivational triggers?

Motivational Triggers; is the ability of an attacker to trigger a user into doing something for them.

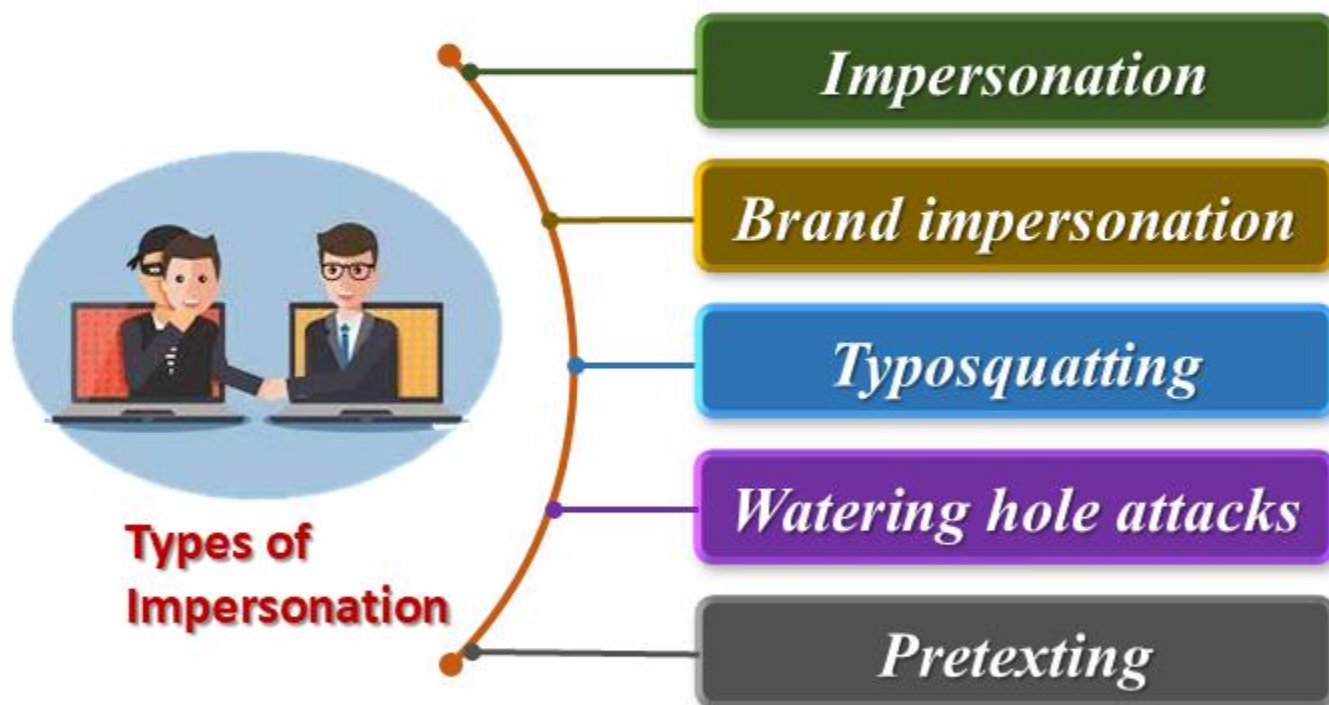


- **Authority;** is the *power to give orders* or make decisions and enforce obedience.
- **Urgency;** is the *sense of time sensitivity* that drives individuals to act swiftly or prioritize certain actions.
- **Social Proof;** is a psychological phenomenon where individuals *look to the behaviors and actions of others* to determine their own decisions and actions in similar situations.

- **Scarcity;** is the *psychological pressure* people feel when they believe a product, opportunity or *resource is limited or in short supply*.
- **Likability;** is when the attacker *being nice, friendly, and socially accepted* by the others, it usually *done by sexual attraction, pretending to be a friend, or common interest*.
- **Fear;** is being afraid of someone or something, as likely to be dangerous, painful, or threatening.

What is Impersonation?

Impersonation; is the act of attempting to deceive someone by *pretending that you are another person.*

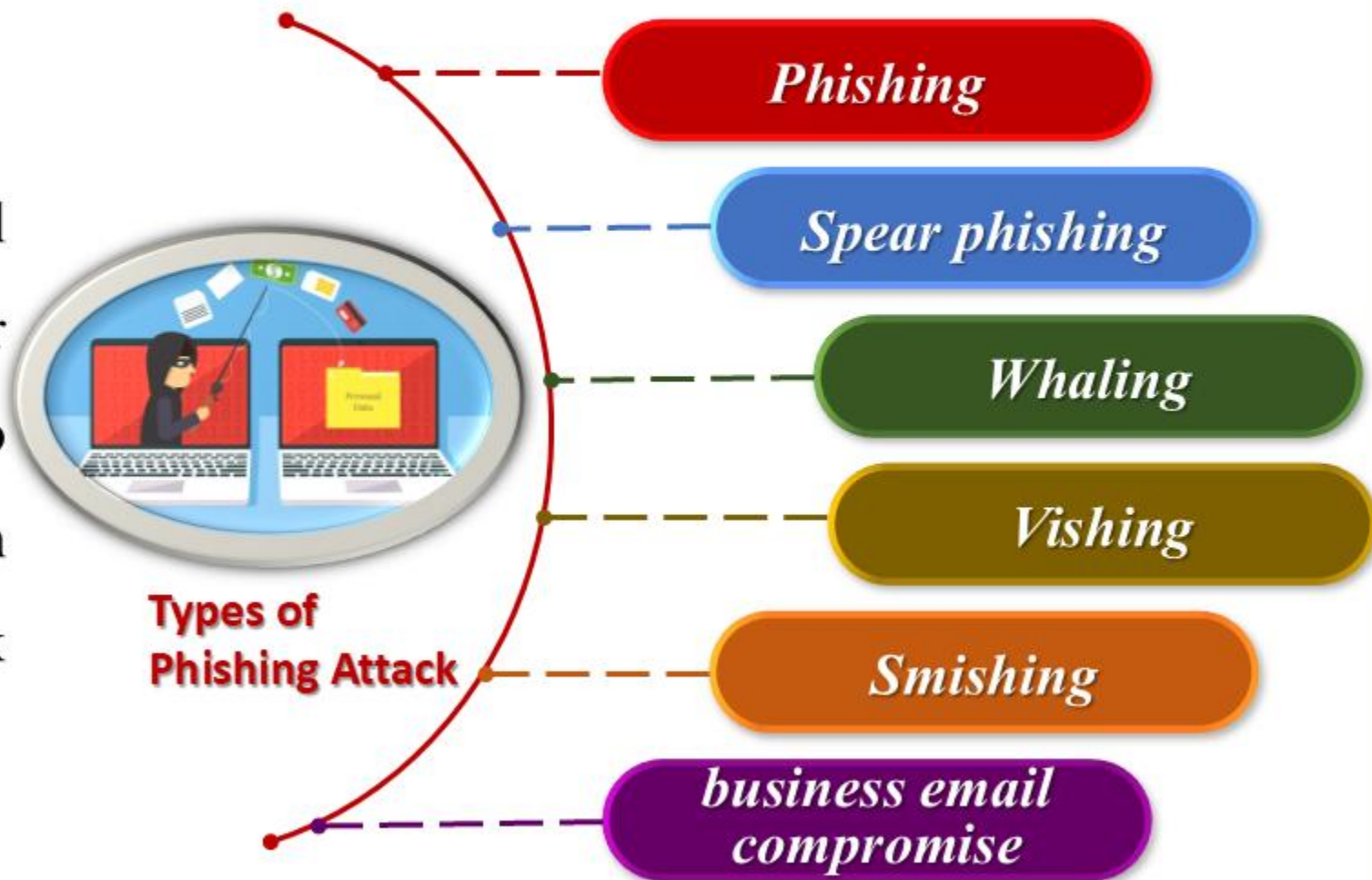


- **Impersonation;** is refers to an attack where an attacker assumes the identity of another person to gain unauthorized access to resources or steal sensitive data.
- **Brand impersonation;** is where an attacker pretends to represent a legitimate company or brand.
- **Typosquatting;** also known as *URL hijacking or cyber-squatting*, a form of cyber attack where an attacker *registers a domain name that is similar to a popular website* but contains some of the common typographical errors.

- ***Watering hole attacks;*** is a security exploit in which the attacker seeks to compromise a specific group of end users by *infecting websites or services* that members of the group are known to visit or use.
- ***Pretexting;*** is a certain type of social engineering technique which an attacker tries to convince a victim to give up valuable information or access to a service or system.

What is Phishing Attack?

Phishing Attack; is a criminal mechanism that use of email or websites for tricking users into giving personal information such as ID, Credit data, financial bank account credentials etc.



- **Phishing;** is an attack that involves *sending fraudulent emails that appear to be from a reputable source*, with the aim of convincing individuals to reveal personal information such as passwords or credit card numbers.
- **Spear phishing;** is a *more targeted form of phishing* that is used by cyber criminals who are more tightly *focused on a specific group of individuals or organizations*.
- **Whaling;** is a form of spear phishing that targets high profile individuals like CEOs or CFOs.

- **Vishing, or Voice phishing;** is an attack where an attacker tricks their victims into *sharing personal or financial information over the phone*.
- **Smishing or SMS phishing;** is an attack that involves the *use of text messages to trick individuals* into providing their personal information.
- **Business email compromise;** is a sophisticated type of phishing attack that usually targets businesses by *using one of their internal email accounts* to get other employees to perform some kind of malicious action on behalf of the attacker.

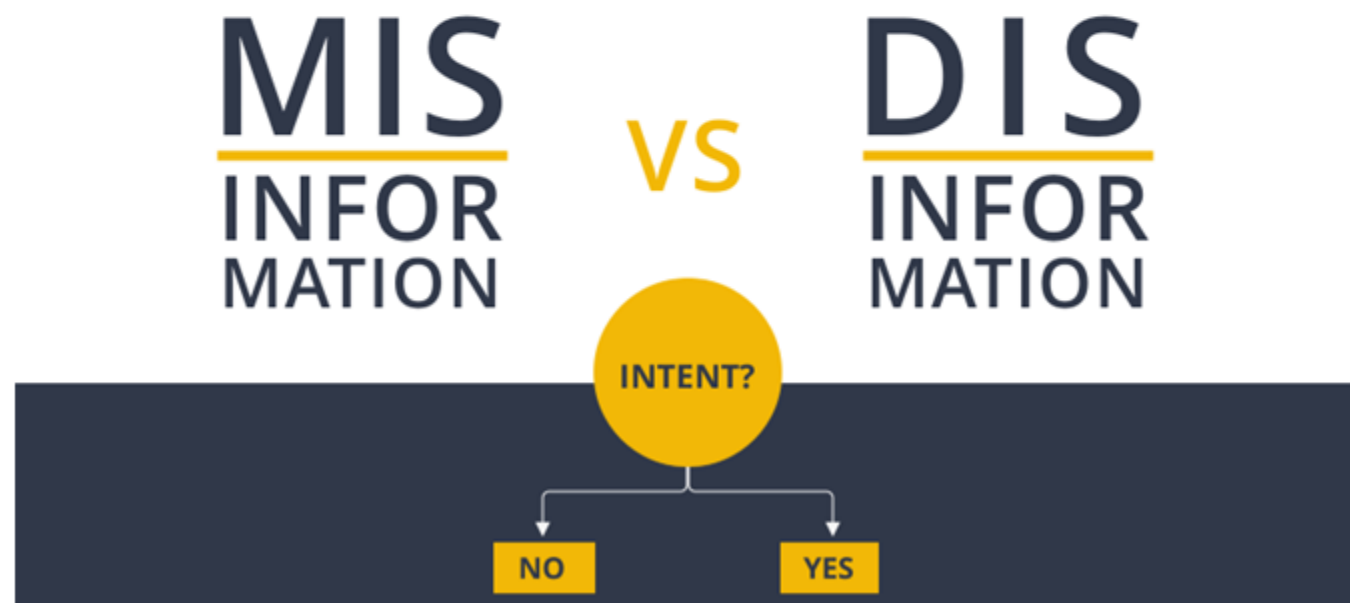
What is difference between Fraud and Scam?

- **Fraud;** is *unauthorized access to personal information without the victim's knowledge* or permission. (e.g., Identity theft, Unauthorized credit card use, Insurance fraud, etc.)
- **Scam;** is *manipulate victims into willingly providing their information*. (e.g., Prize scams, invoice scam, etc.)



What is difference Misinformation and Disinformation?

- **Misinformation;** is *false information that is spread*, without harmful intent.
- **Disinformation;** is *false information that is spread*, with the intent to deceive or mislead.



What is an Anti-phishing Campaign?

An anti-phishing campaign; is an essential user *security awareness training tool* that can be used to *educate individuals about the risk of phishing* and how to best identify potential phishing attempts.

Training involves identifying individuals about different phishing techniques and how to identify *urgency, unusual requests, mismatched URLs, strange email addresses,* and *poor spelling or grammar* being used in the emails received from an attacker. Using tool like *(Phish Insights) by Trend Micro.*

- ***Diversion Theft;*** is stealing sensitive data by tricking the victim into sending it to or sharing it with the wrong person. (e.g., DNS Spoofing).
- ***A hoax;*** is a *malicious deception* that is often spread through social media, email, or other communication channels *used to spread malware or phishing attacks*.
- ***Shoulder surfing;*** is looking over someone's shoulder to gather personal information. (e.g., steal PINs at ATMs, passwords on public computers, etc.)
- ***Dumpster diving;*** is *searching through trash* to find valuable information.

Common Social Engineering Attacks

- **Eavesdropping;** the process of *secretly listening to private conversations*.
- **Baiting;** is *leaving a malware-infected physical device*, like a USB drive, in a place where it will be found by a victim who will then hopefully use the device to unknowingly install malware on the organization's computer system.
- **Piggybacking or Tailgating;** is the unauthorized person following an authorized person into a secure area. **In Tailgating;** the attacker attempts to *follow an employee* through an access control vestibule or access control point *without their knowledge*, while **in Piggybacking;** the attacker *convincing an authorized employee to let them into the facility* by getting the *authorized employee to swipe their own access badge*.

What is Malware?

Malware; is any *program designed to intentionally be harmful to a computer*, network or server without the user's knowledge or permission.

For the malware to infect your system, it needs to be able to create a *threat vector* and an *attack vector*.



- **Computer Virus;** is a *malicious code* that's run on a machine without the user's knowledge, and this allows the code to infect the computer whenever it has been run and start *performing some malicious activities*, including replicating across your network, deleting your critical files, and using a valuable computing resources within your systems.
- **Boot sector virus;** is going to be *stored in the first sector of a hard disk* or solid-state device and is then *loaded into memory whenever that can computer boots up*.
 - **Macro virus;** is a form of code that *allows a virus to be embedded inside another document* so that when that document is open by the user, the virus will then be executed.

- **Program virus;** is *executables or application files* to infect with their malicious code.
- **Multipartite virus;** is a *combination of a boot sector type of virus and a program type of virus*. By using this combination, the virus can place itself in the boot sector and then get loaded up every time the computer boots, it can then install itself within a program where it can be run every time the computer starts up because that program is always started whenever the computer is booted up.
- **Encrypted virus;** is designed to *hide itself from being detected by encrypting its malicious code* or payloads To avoid detection by any anti-virus software.

- **Polymorphic viruses;** is an advanced version of an encrypted virus, but instead of just encrypting the contents, it's going to *change the virus's code each time it's executed* by altering the decryption module to evade detection (*create modified versions of itself*).
- **Metamorphic virus;** is a more advanced version of a polymorphic virus, it can write itself entirely before it attempts to infect a given file (*ability to translate, edit and rewrite its own code*).
- **Stealth virus;** is using different techniques to avoid detection by an anti-virus software, including things like encrypting its contents, modifying its payload, and other methods to avoid detection.

- **Armored viruses;** have a *layer of protection* that confuse a program or a person who's trying to analyze it.
- **A hoax;** is a form of technical social engineering that attempts to *scare our end users into taking some kind of undesirable action on their system.*
- **Computer worm;** is a piece of malicious software, much like a virus, that *can replicate itself* without any user intervention.

- **Trojan;** is a piece of malicious software that is disguised as a piece of harmless or desirable software. a **RAT** is a type of Trojan that provides the attacker with remote control of a victimized machine.
- **Ransomware;** is a type of malware that *locks and encrypts a victim's data*, files, devices or systems, rendering them inaccessible and unusable until the attacker receives a ransom payment. To mitigate against ransomware using *regular backup, updates, and implementing multi-factor authentication for the systems.*

- **Botnet;** is a *network of compromised computers or devices controlled remotely by malicious actors* and they're often used for cyber attacks or other malicious activities.
- **Zombies;** is the name of a compromised computer or device that is part of a botnet and used to *perform tasks using remote commands from the attacker without the user's knowledge*.
- **Rootkit;** is a specific type of software that's designed to *gain administrative-level control, over a given computer system without being detected*. For rootkit detection removal is going to be to *conduct an external system scan*.

- **Backdoor;** is originally placed into computer programs to *bypass the normal security and authentication functions of those systems.*
- **Keylogger;** is a type of surveillance technology used to *monitor and record each keystroke on a specific device*, such as a computer or smartphone. It can be either hardware- or software-based.
- **Spyware;** is the type of malicious software that's designed to *gather and send information about a user or organization without their knowledge.*

➤ **Bloatware;** is *any software that comes pre-installed on your new computer or smartphone* that you, as the user, did not specifically request, want or need.

In general, *bloatware is not going to be malicious*, but it does *waste your storage space, slows down the performance* of your devices and *introduces new security vulnerabilities* into your systems.

- **Account lockouts;** malware, especially those designed for credential theft or brute force attacks, will *trigger multiple failed login attempts* that could result in a *user's account being locked out*.
- **Concurrent session utilization;** *one user typically only have one active session at any given time* inside of our network. If you notice that a *single user account has multiple simultaneous or concurrent sessions open*, especially from various geographic locations, this should really be a cause for concern and suspicion.

- **Blocked content;** If there's a *sudden increase in the amount of blocked content alerts you're seeing from your security tools*, this is a strong indication that a malware infection may have successfully penetrated your system.
- **Impossible travel;** where a user's account is *accessed from two or more geographically separated locations* in an impossibly short period of time.
- **Resource consumption;** observing any *unusual spikes in CPU, memory, or network bandwidth utilization* that can't be linked back to a legitimate task, that could be an indication that you're the victim of a malware attack.

- **Resource inaccessibility;** if you have *a large number of files or critical systems that are suddenly inaccessible to you*, Or if users *receive messages demanding payment to decrypt their data*, this is a pretty clear sign of a ransomware-based malware attack.
- **Out-of-cycle logging;** If you're noticing that *your logs are being generated at odd hours*, or during times when no legitimate activities should have been taking place.
- **Missing logs;** if you're conducting a log review as a cybersecurity analyst, and *you see there's a large gap in your logs*, threat actor or attacker will delete your system logs in order to hide their own tracks after successfully breaching your system.

