2024 - 2025

IAGI - 1

# Cybersecurity

# Introduction

Pr. Mouaad MOHY-EDDINE

mohy-eddine.mouaad@ensam-casa.ma

# Table de Contenu

Introduction

Définitions

Utilisateurs

Serveurs

Machine de Transport

Attentes

Rôles

Niveaux de Décisions

Pr. Mouaad MOHY-EDDINE

mohy-eddine.mouaad@ensam-casa.ma

# Introduction

# Introduction

Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. As we’ve already seen, they are interested in **everything**, from credit cards to product designs!

# Types of Attackers

Let’s look at some of the main types of cyber attackers who’ll try anything to get their hands on our information. They are often categorized as **white hat**, **gray hat** or **black hat** attackers.

# Types of Attackers

Let’s look at some of the main types of cyber attackers who’ll try anything to get their hands on our information. They are often categorized as **white hat**, **gray hat** or **black hat** attackers.

# Types of Attackers

Let’s look at some of the main types of cyber attackers who’ll try anything to get their hands on our information. They are often categorized as **white hat**, **gray hat** or **black hat** attackers.

***Amateurs***

The term 'script kiddies' emerged in the 1990s and refers to amateur or inexperienced hackers who use existing tools or instructions found on the Internet to launch attacks. Some script kiddies are just curious, others are trying to demonstrate their skills and cause harm. While script kiddies may use basic tools, their attacks can still have devastating consequences.

# Types of Attackers

Let’s look at some of the main types of cyber attackers who’ll try anything to get their hands on our information. They are often categorized as **white hat**, **gray hat** or **black hat** attackers.

### *Hackers*

This group of attackers break into computer systems or networks to gain access. Depending on the intent of their break in, they can be classified as white, gray or black hat hackers.

- **White hat attackers** break into networks or computer systems to identify any weaknesses so that the security of a system or network can be improved. These break-ins are done with prior permission and any results are reported back to the owner.
- **Gray hat attackers** may set out to find vulnerabilities in a system but they will only report their findings to the owners of a system if doing so coincides with their agenda. Or they might even publish details about the vulnerability on the internet so that other attackers can exploit it.
- **Black hat attackers** take advantage of any vulnerability for illegal personal, financial or political gain.

# Types of Attackers

Let's look at some of the main types of cyber attackers who'll try anything to get their hands on our information. They are often categorized as **white hat**, **gray hat** or **black hat** attackers.

***Organized hackers***

These attackers include organizations of cyber criminals, hacktivists, terrorists and state-sponsored hackers. They are usually highly sophisticated and organized, and may even provide cybercrime as a service to other criminals.

**Hacktivists** make political statements to create awareness about issues that are important to them.

**State-sponsored attackers** gather intelligence or commit sabotage on behalf of their government. They are usually highly trained and well-funded and their attacks are focused on specific goals that are beneficial to their government.

# What Color Is My Hat?

Now that you know the different types of attackers and their motivations for doing what they do, can you identify what color of hat is worn by the attacker in each of the following scenarios? This is a tricky one but remember, you can earn valuable defender points if you answer correctly.

After hacking into ATM systems remotely using a laptop, this attacker worked with the ATM manufacturers to resolve the identified security vulnerabilities.

A. Gray Hat
B. White Hat
C. Black Hat

# What Color Is My Hat?

Now that you know the different types of attackers and their motivations for doing what they do, can you identify what color of hat is worn by the attacker in each of the following scenarios? This is a tricky one but remember, you can earn valuable defender points if you answer correctly.

This attacker transferred $10 million into their bank account using customer account and PIN credentials gathered from recordings.

A. Gray Hat
B. White Hat
C. Black Hat

# What Color Is My Hat?

Now that you know the different types of attackers and their motivations for doing what they do, can you identify what color of hat is worn by the attacker in each of the following scenarios? This is a tricky one but remember, you can earn valuable defender points if you answer correctly.

This attacker’s job is to identify weaknesses in a company’s computer system.

A. Gray Hat
B. White Hat
C. Black Hat

# What Color Is My Hat?

Now that you know the different types of attackers and their motivations for doing what they do, can you identify what color of hat is worn by the attacker in each of the following scenarios? This is a tricky one but remember, you can earn valuable defender points if you answer correctly.

This attacker used malware to compromise a company’s system and steal credit card information that was then sold to the highest bidder.

A. Gray Hat
B. White Hat
C. Black Hat

# What Color Is My Hat?

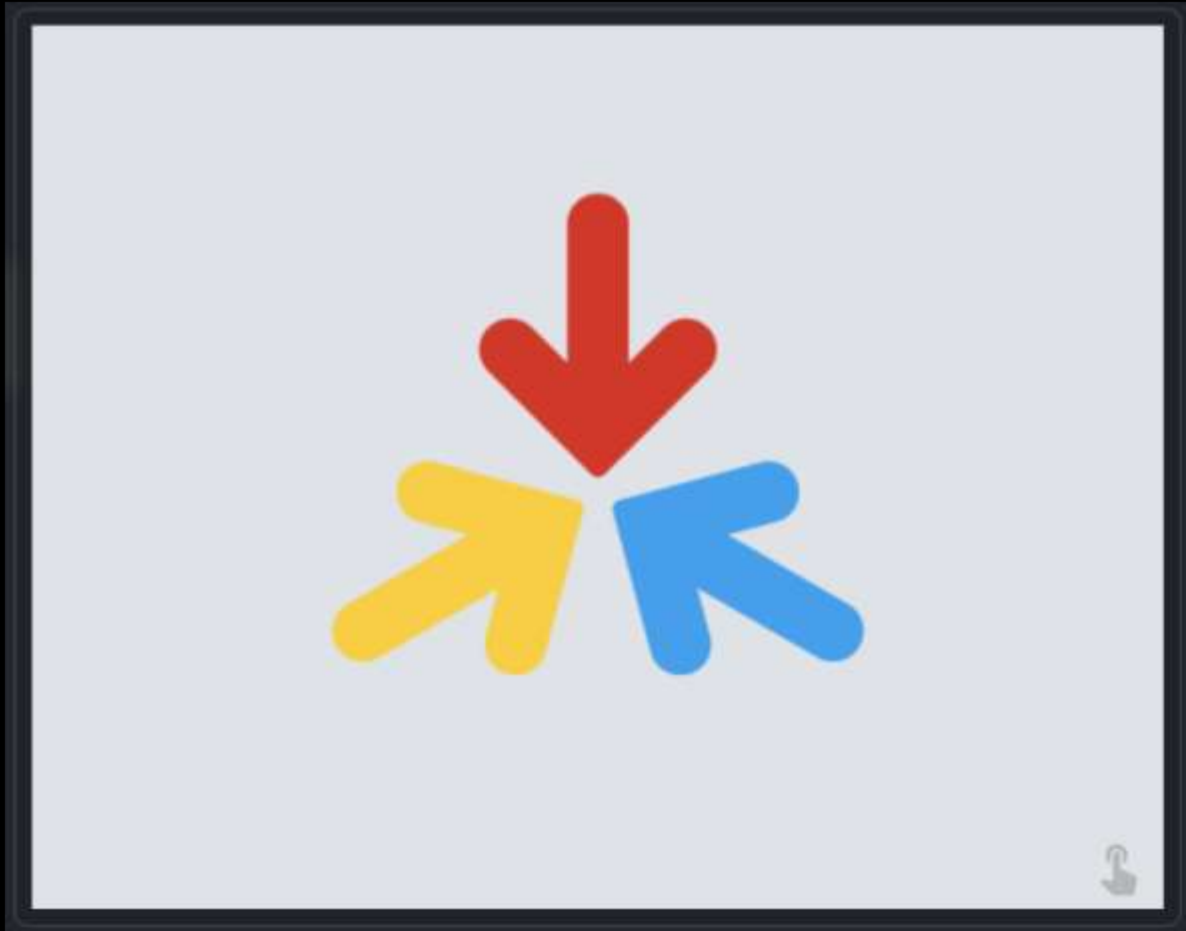
Now that you know the different types of attackers and their motivations for doing what they do, can you identify what color of hat is worn by the attacker in each of the following scenarios? This is a tricky one but remember, you can earn valuable defender points if you answer correctly.

While carrying out some research, this attacker stumbled across a security vulnerability on an organization's network that they are authorized to access.

A. Gray Hat
B. White Hat
C. Black Hat

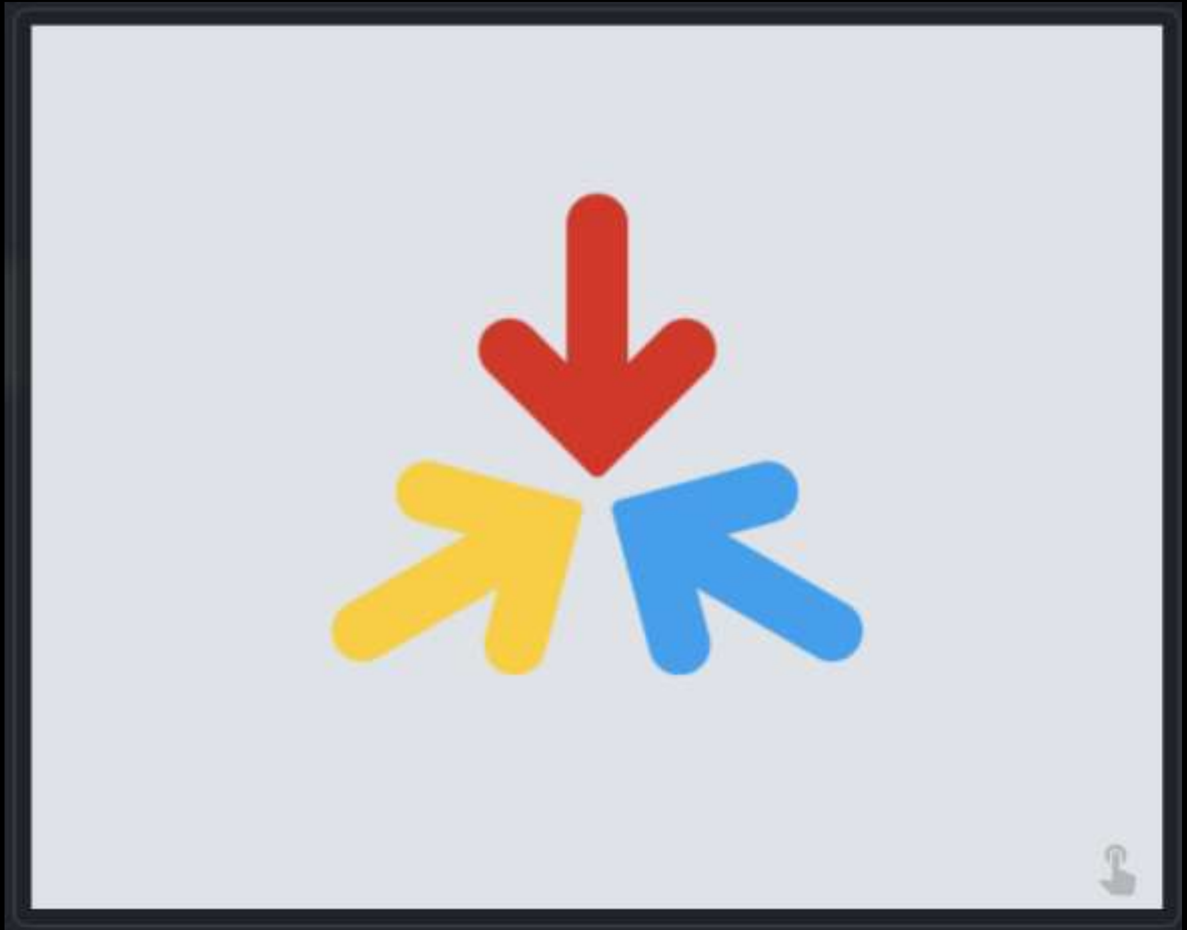
# Internal and External Threats

Cyber attacks can originate from within an organization as well as from outside of it.



# Internal and External Threats

Cyber attacks can originate from within an organization as well as from outside of it.



***Internal***

Employees, contract staff or trusted partners can accidentally or intentionally:

- Mishandle confidential data.
- Facilitate outside attacks by connecting infected USB media into the organization’s computer system.
- Invite malware onto the organization’s network by clicking on malicious emails or websites.
- Threaten the operations of internal servers or network infrastructure devices.

# Internal and External Threats

Cyber attacks can originate from within an organization as well as from outside of it.

***External***

Amateurs or skilled attackers outside of the organization can:

- Exploit vulnerabilities in the network.
- Gain unauthorized access to computing devices.
- Use social engineering to gain unauthorized access to organizational data.

# What Do You Think?

Remember that phishing email you received earlier from one of your customers?

An investigation into this email revealed that the user accounts and access privileges of a former employee were not fully removed from the IT systems on leaving the company. In fact, this former employee, who now works for a competitor, logged into @Apollo’s customer database only three days ago.

**Has an internal or external security threat occurred here?**

## What Do You Think?

✓

Remember that phishing email you received earlier from one of your customers?

An investigation into this email revealed that the user accounts and access privileges of a former employee were not fully removed from the IT systems on leaving the company. In fact, this former employee, who now works for a competitor, logged into @Apollo’s customer database only three days ago.

**Has an internal or external security threat occurred here?**

**Internal**

# Cyberwarfare

# Cyberwarfare

Cyberwarfare, as its name suggests, is the use of technology to penetrate and attack another nation’s computer systems and networks in an effort to cause damage or disrupt services, such as shutting down a power grid.

***Sign of the Times (Stuxnet)***

One example of a state-sponsored attack involved the Stuxnet malware that was designed not just to hijack targeted computers but to actually cause physical damage to equipment controlled by computers!

# Cyberwarfare

The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

# The Purpose of Cyberwarefare

The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

**To gather compromised information and/or defense secrets**

A nation or international organization can engage in cyberwarfare in order to steal defense secrets and gather information about technology that will help narrow the gaps in its industries and military capabilities.

Furthermore, compromised sensitive data can give attackers leverage to blackmail personnel within a foreign government.

# The Purpose of Cyberwarefare

The main reason for resorting to cyberwarfare is to gain advantage over adversaries, whether they are nations or competitors.

## To impact another nation’s infrastructure

Besides industrial and military espionage, a nation can continuously invade another nation’s infrastructure in order to cause disruption and chaos.

For example, a cyber attack could shut down the power grid of a major city. Consider the consequences if this were to happen; roads would be congested, the exchange of goods and services would be halted, patients would not be able to get the care they would need if an emergency occurred, access to the internet would be interrupted. By shutting down a power grid, a cyber attack could have a huge impact on the everyday life of ordinary citizens.

# The Purpose of Cyberwarefare

Cyberwarfare can destabilize a nation, disrupt its commerce, and cause its citizens to lose faith and confidence in their government without the attacker ever physically setting foot in the targeted country.

# The Purpose of Cyberwarefare

Cyberwarfare can destabilize a nation, disrupt its commerce, and cause its citizens to lose faith and confidence in their government without the attacker ever physically setting foot in the targeted country.

# Analyzing a Cy
Attack

# Analyzing a Cyber Attack

Cybercriminals use many different types of malicious software, or malware, to carry out their activities. Malware is any code that can be used to steal data, bypass access controls, or cause harm to or compromise a system. Knowing what the different types are and how they spread is key to containing and removing them.

# Type of Malware

## SPYWARE

Designed to track and spy on you, spyware monitors your online activity and can log every key you press on your keyboard, as well as capture almost any of your data, including sensitive personal information such as your online banking details. Spyware does this by modifying the security settings on your devices.

It often bundles itself with legitimate software or Trojan horses.

# Type of Malware

Adware is often installed with some versions of software and is designed to automatically deliver advertisements to a user, most often on a web browser. You know it when you see it! It’s hard to ignore when you’re faced with constant pop-up ads on your screen.
It is common for adware to come with spyware.

# Type of Malware

## BACKDOOR

This type of malware is used to gain unauthorized access by bypassing the normal authentication procedures to access a system. As a result, hackers can gain remote access to resources within an application and issue remote system commands.

A backdoor works in the background and is difficult to detect.

# Type of Malware

This malware is designed to hold a computer system or the data it contains captive until a payment is made. Ransomware usually works by encrypting your data so that you can’t access it.

Some versions of ransomware can take advantage of specific system vulnerabilities to lock it down. Ransomware is often spread through phishing emails that encourage you to download a malicious attachment or through a software vulnerability.

# Type of Malware

This is a type of malware that uses 'scare’ tactics to trick you into taking a specific action. Scareware mainly consists of operating system style windows that pop up to warn you that your system is at risk and needs to run a specific program for it to return to normal operation.

If you agree to execute the specific program, your system will become infected with malware.

# Type of Malware

This malware is designed to modify the operating system to create a backdoor, which attackers can then use to access your computer remotely. Most rootkits take advantage of software vulnerabilities to gain access to resources that normally shouldn’t be accessible (privilege escalation) and modify system files.

Rootkits can also modify system forensics and monitoring tools, making them very hard to detect. In most cases, a computer infected by a rootkit has to be wiped and any required software reinstalled.

## Type of Malware

A virus is a type of computer program that, when executed, replicates and attaches itself to other executable files, such as a document, by inserting its own code. Most viruses require end-user interaction to initiate activation and can be written to act on a specific date or time.

Viruses can be relatively harmless, such as those that display a funny image. Or they can be destructive, such as those that modify or delete data.

Viruses can also be programmed to mutate in order to avoid detection. Most viruses are spread by USB drives, optical disks, network shares or email.

# Type of Malware

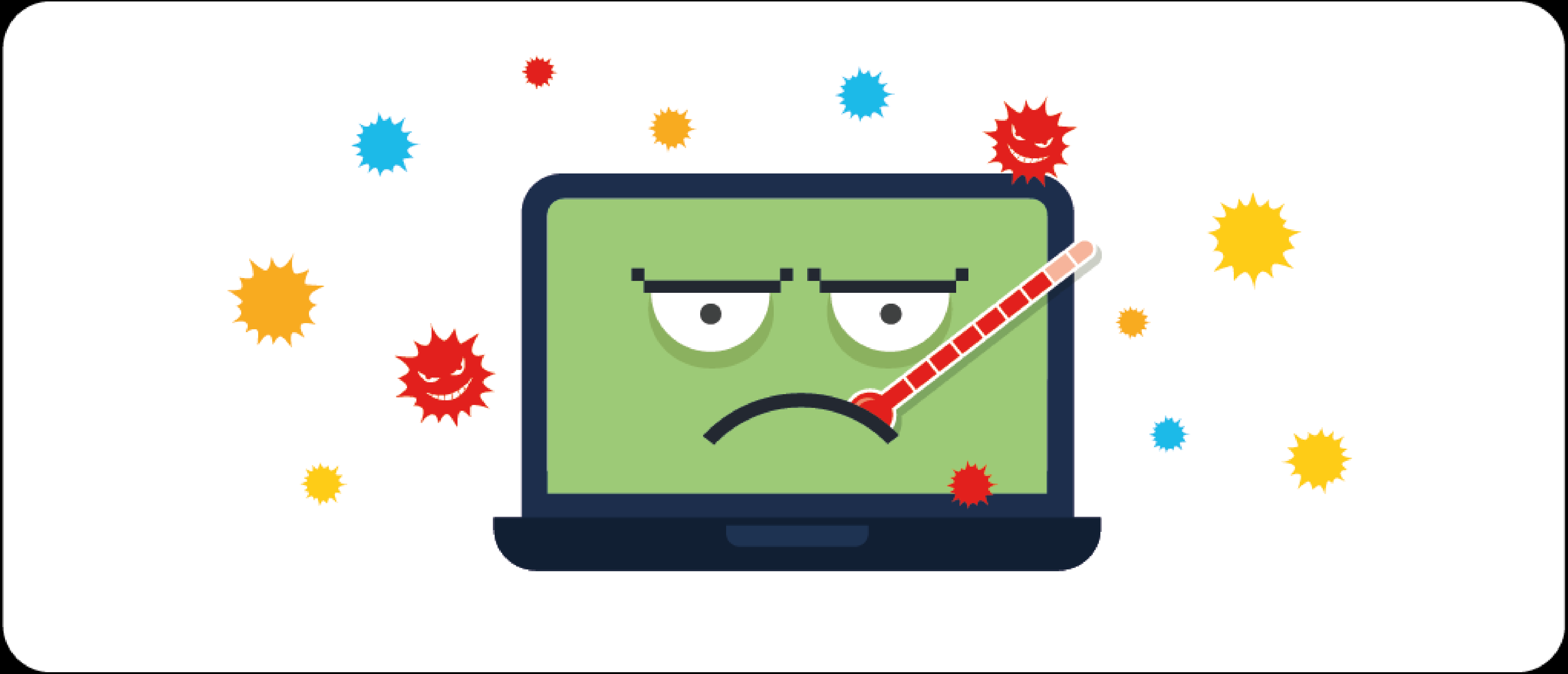
This is a type of malware that replicates itself in order to spread from one computer to another. Unlike a virus, which requires a host program to run, worms can run by themselves. Other than the initial infection of the host, they do not require user participation and can spread very quickly over the network.

Worms share similar patterns: They exploit system vulnerabilities, they have a way to propagate themselves, and they all contain malicious code (payload) to cause damage to computer systems or networks.

Worms are responsible for some of the most devastating attacks on the Internet. In 2001, the Code Red worm had infected over 300,000 servers in just 19 hours.

# Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?



# Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Regardless of the type of malware a system has been infected with, there are some common symptoms to look out for. These include:

- ✓ an increase in central processing unit (CPU) usage, which slows down your device.
- ✓ your computer freezing or crashing often.
- ✓ a decrease in your web browsing speed.
- ✓ unexplainable problems with your network connections.
- ✓ modified or deleted files.
- ✓ the presence of unknown files, programs or desktop icons.
- ✓ unknown processes running.
- ✓ programs turning off or reconfiguring themselves.
- ✓ emails being sent without your knowledge or consent.

# Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Malware designed to track your online activity and capture your data

A. Adware
B. Ransomware
C. Spyware

## Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Software that automatically delivers advertisements

A. Worms
B. Ransomware
C. Adware

## Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Malware that holds a computer system captive until a payment is made to the attacker

A. Worms
B. Ransomware
C. Virus

# Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Malicious code that attaches to legitimate programs and usually spreads by USB drives, optical media, network shares or email

A. Adware
B. Virus
C. Spyware

# Symptoms of Malware

So now you know about the different kinds of malware. But what do you think their symptoms might be?

Malicious code that replicates itself independently by exploiting vulnerabilities in networks

A. Virus
B. Worm
C. Adware

# Methods of Infiltration

Methods of Infiltration

## Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people’s willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee’s vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

# Methods of Infiltration

## Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people’s willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee’s vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

**Pretexting**
This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data.
For example, pretending to need a person’s personal or financial data in order to confirm their identity.

## Social Engineering

**DEFCON h4cker shows her skills in social engineering !**

I bet they have my back. But yes, go for it.

# Methods of Infiltration

## Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people’s willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee’s vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

**Tailgating**
This is when an attacker quickly follows an authorized person into a secure, physical location.

# Methods of Infiltration

## Social Engineering

Social engineering is the manipulation of people into performing actions or divulging confidential information. Social engineers often rely on people's willingness to be helpful, but they also prey on their weaknesses. For example, an attacker will call an authorized employee with an urgent problem that requires immediate network access and appeal to the employee's vanity or greed or invoke authority by using name-dropping techniques in order to gain this access.

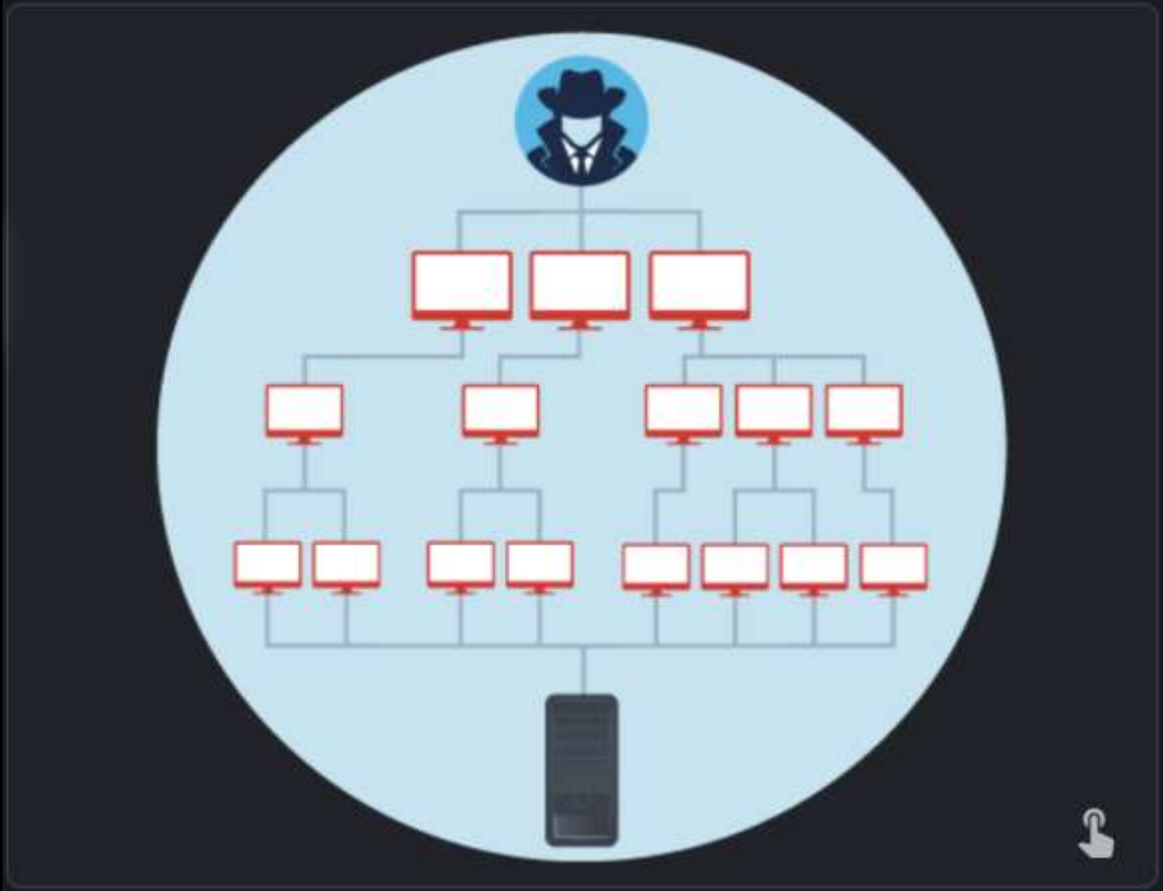
**Something for something (quid pro quo)**
This is when an attacker requests personal information from a person in exchange for something, like a free gift.

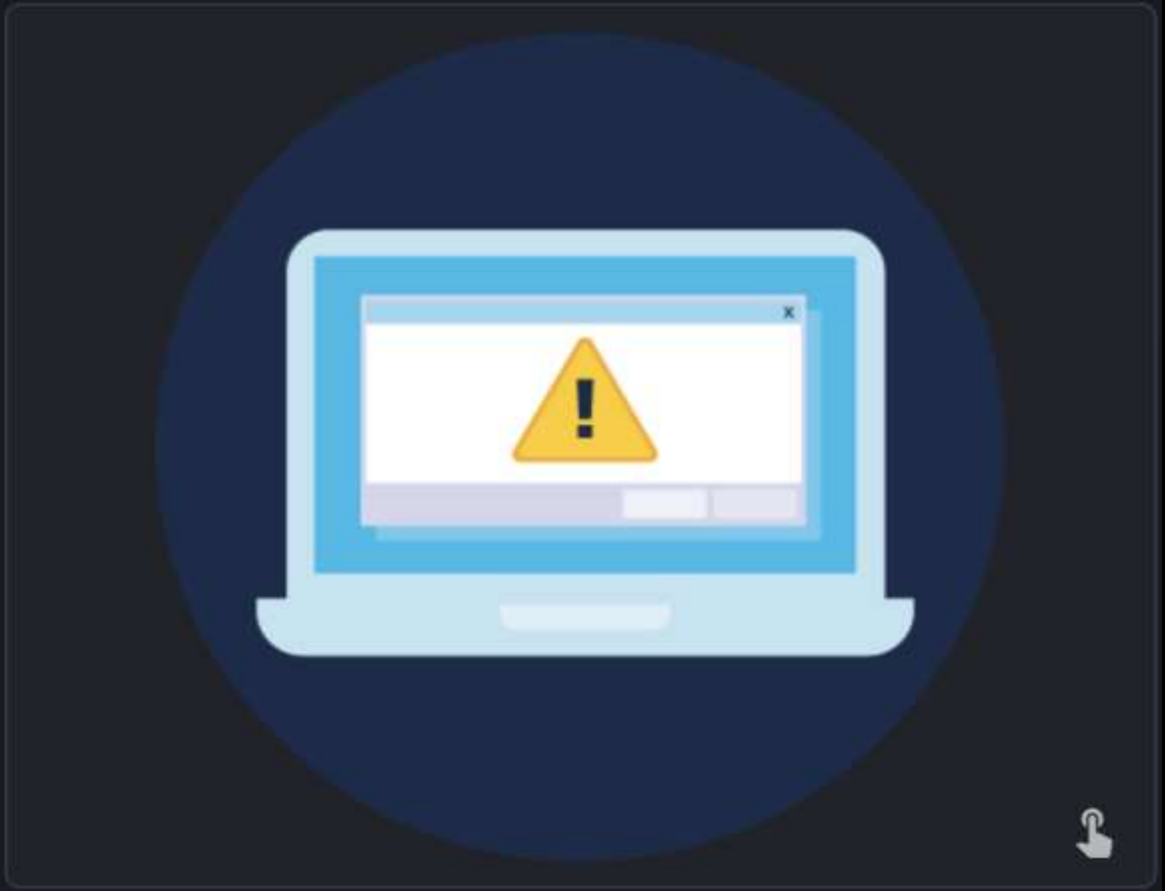
## Denial-of-Service (DoS)

Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications.

## Denial-of-Service (DoS)

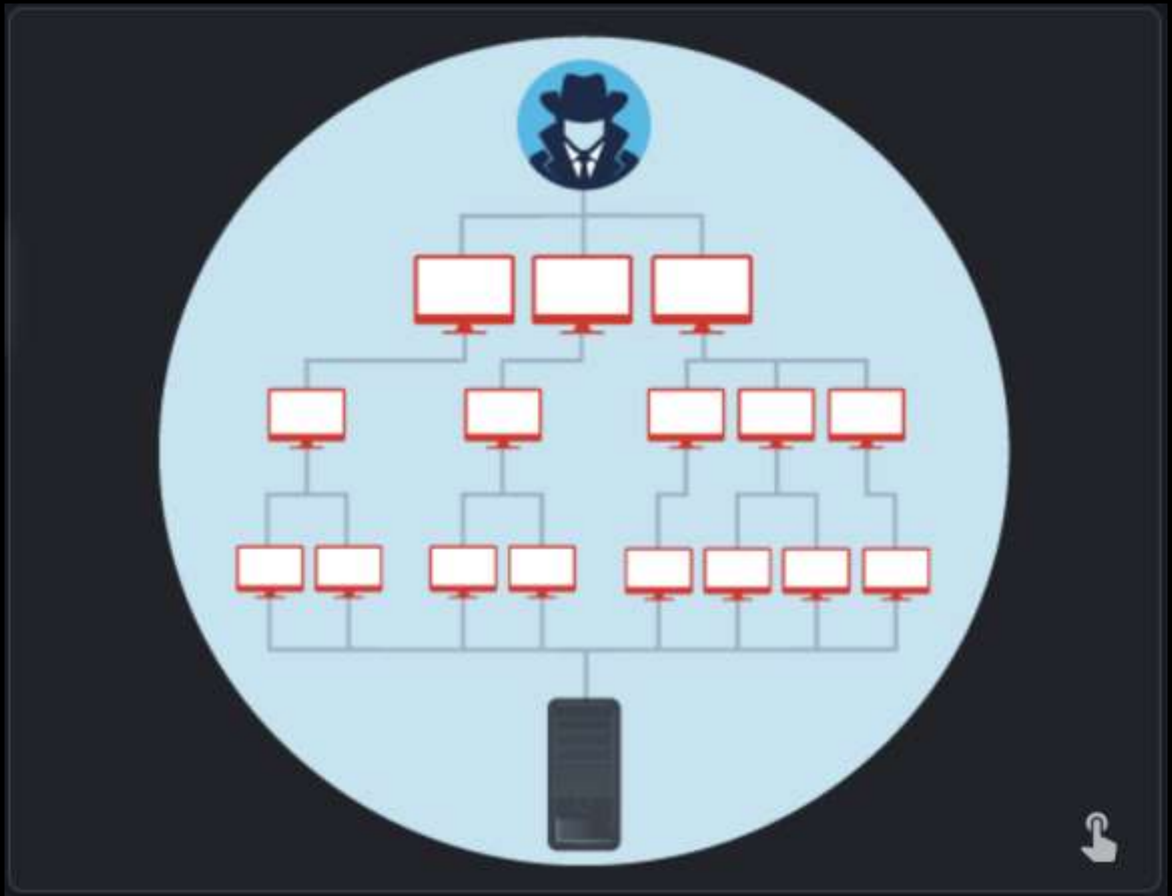
Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications.





## Denial-of-Service (DoS)

Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications.



**Overwhelming quantity of traffic**

This is when a network, host or application is sent an enormous amount of data at a rate which it cannot handle. This causes a slowdown in transmission or response, or the device or service to crash.

Methods of Infiltration

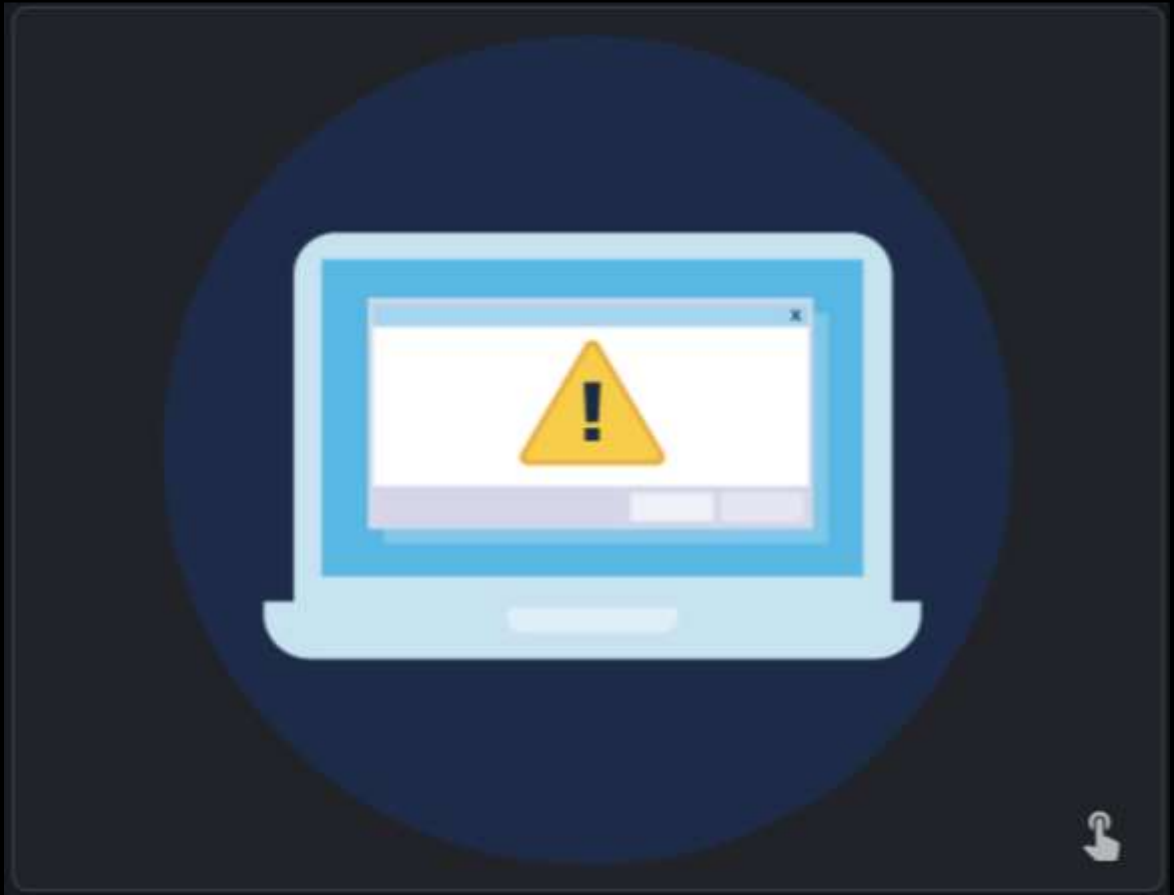
## Denial-of-Service (DoS)

Denial-of-Service (DoS) attacks are a type of network attack that is relatively simple to carry out, even by an unskilled attacker. A DoS attack results in some sort of interruption of network service to users, devices or applications.

**Maliciously formatted packets**

A packet is a collection of data that flows between a source and a receiver computer or application over a network, such as the Internet. When a maliciously formatted packet is sent, the receiver will be unable to handle it.

For example, if an attacker forwards packets containing errors or improperly formatted packets that cannot be identified by an application, this will cause the receiving device to run very slowly or crash.

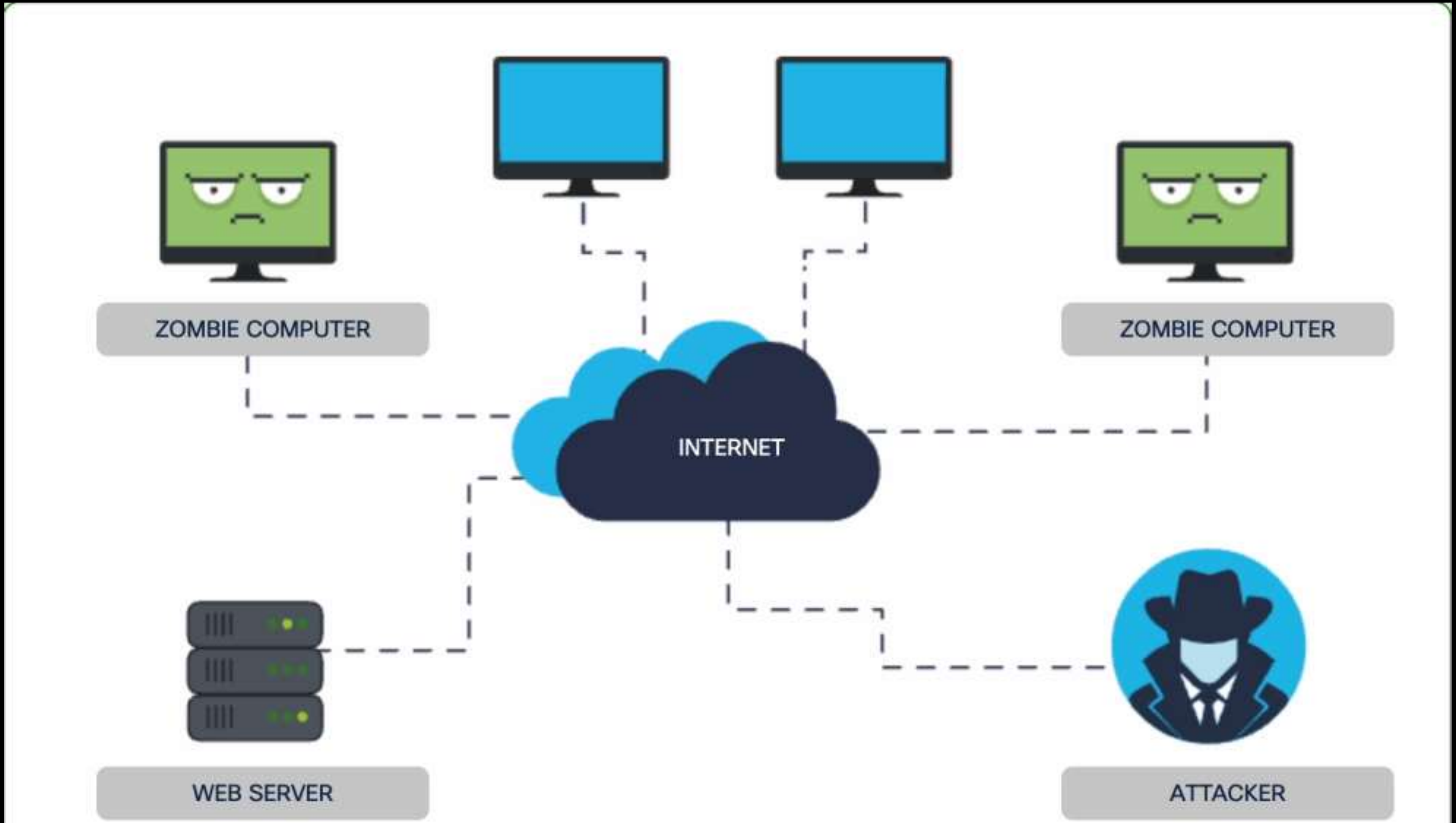


## Distributed DoS

A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources. For example:

- An attacker builds a network (botnet) of infected hosts called zombies, which are controlled by handler systems.
- The zombie computers will constantly scan and infect more hosts, creating more and more zombies.
- When ready, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

## Distributed DoS



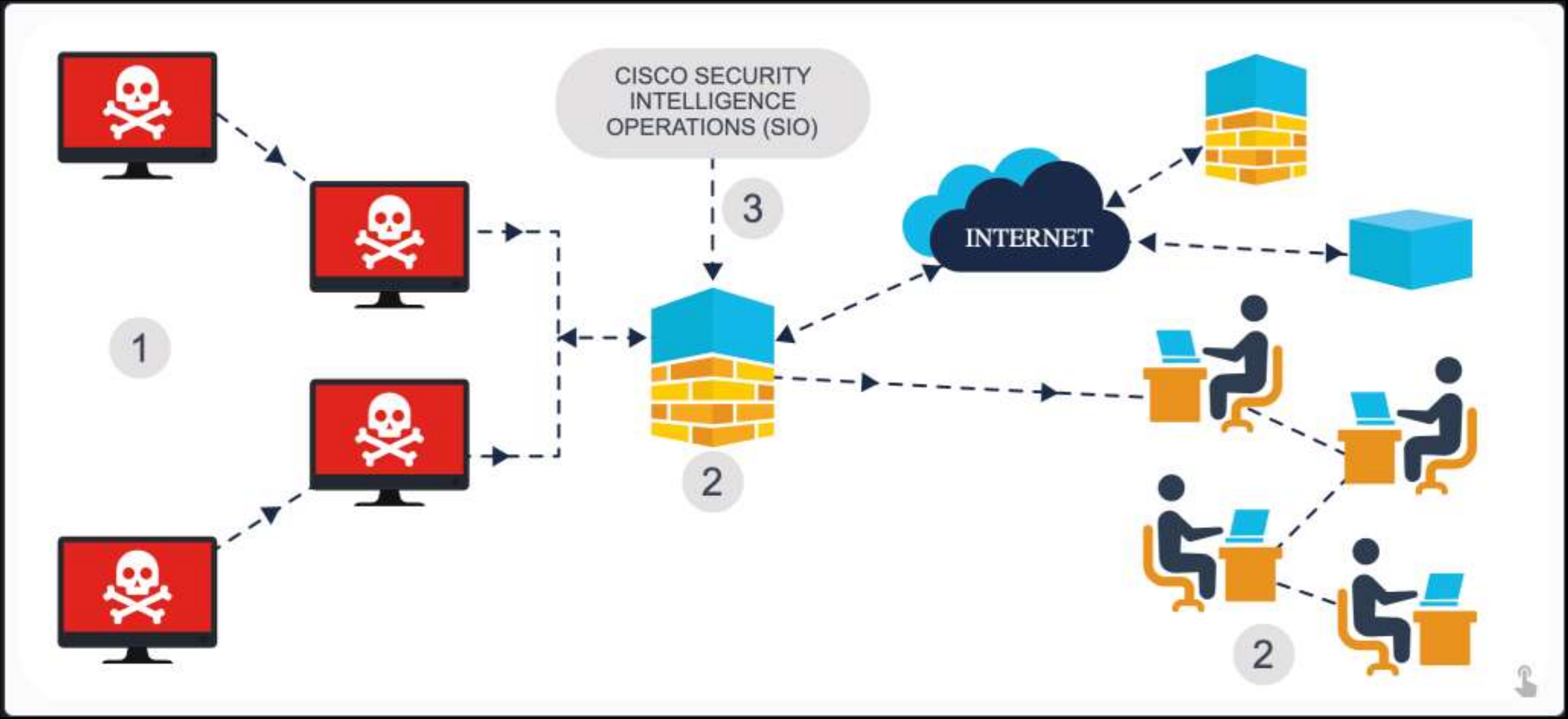
## Botnet

A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or infected media file. A botnet is a group of bots, connected through the Internet, that can be controlled by a malicious individual or group. It can have tens of thousands, or even hundreds of thousands, of bots that are typically controlled through a command and control server.

These bots can be activated to distribute malware, launch DDoS attacks, distribute spam email, or execute brute-force password attacks. Cybercriminals will often rent out botnets to third parties for nefarious purposes.

Methods of Infiltration

## Botnet



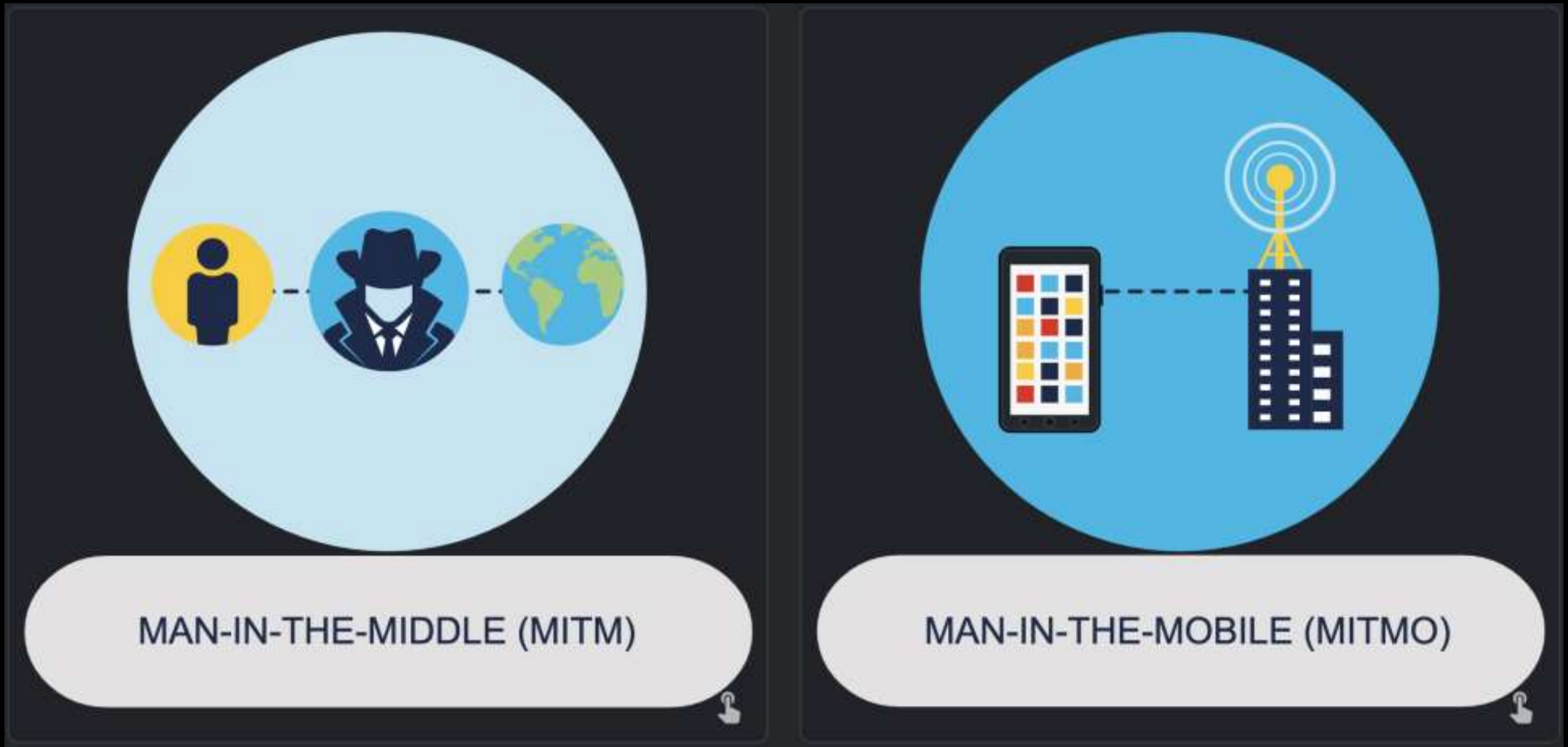
## On-Path Attacks

On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices.

This type of attack is also referred to as a **man-in-the-middle** or **man-in-the-mobile** attack.

## On-Path Attacks

On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices. This type of attack is also referred to as a **man-in-the-middle** or **man-in-the-mobile** attack.



## On-Path Attacks

On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices. This type of attack is also referred to as a **man-in-the-middle** or **man-in-the-mobile** attack.

MAN-IN-THE-MIDDLE (MITM)

A MitM attack happens when a cybercriminal takes control of a device without the user’s knowledge. With this level of access, an attacker can intercept and capture user information before it is sent to its intended destination. These types of attacks are often used to steal financial information.

There are many types of malware that possess MitM attack capabilities.

Methods of Infiltration

## On-Path Attacks

On-path attackers intercept or modify communications between two devices, such as a web browser and a web server, either to collect information from or to impersonate one of the devices. This type of attack is also referred to as a **man-in-the-middle** or **man-in-the-mobile** attack.

A variation of man-in-middle, MitMo is a type of attack used to take control over a user’s mobile device. When infected, the mobile device is instructed to exfiltrate user-sensitive information and send it to the attackers. ZeuS is one example of a malware package with MitMo capabilities. It allows attackers to quietly capture two-step verification SMS messages that are sent to users.

Methods of Infiltration

## SEO Poisoning

You’ve probably heard of search engine optimization or SEO which, in simple terms, is about improving an organization’s website so that it gains greater visibility in search engine results.

## SEO Poisoning

You’ve probably heard of search engine optimization or SEO which, in simple terms, is about improving an organization’s website so that it gains greater visibility in search engine results.

## SEO Poisoning

You’ve probably heard of search engine optimization or SEO which, in simple terms, is about improving an organization’s website so that it gains greater visibility in search engine results.

Search engines such as Google work by presenting a list of web pages to users based on their search query. These web pages are ranked according to the relevancy of their content.

While many legitimate companies specialize in optimizing websites to better position them, attackers take advantage of popular search terms and use SEO to push malicious sites higher up the ranks of search results. This technique is called SEO poisoning.

The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or attempt social engineering.

✓

## Wi-Fi Password Cracking

You're enjoying your lunch in the canteen when a colleague approaches you. They seem distressed.

They explain that they can't seem to connect to the public Wi-Fi on their phone and ask if you have the private Wi-Fi password to hand so that they can check that their phone is working.

**How would you respond?**

A. "Yes, of course. Give me your phone and I'll put it in for you."
B. "Sure. It's Xgff76dB."
C. "Mmm... I'm not sure we're allowed to use the private Wi-Fi network. Let me check with my manager first."

## Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

## Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

### Password spraying

This technique attempts to gain access to a system by ‘spraying’ a few commonly used passwords across a large number of accounts. For example, a cybercriminal uses 'Password123' with many usernames before trying again with a second commonly-used password, such as ‘qwerty.’

This technique allows the perpetrator to remain undetected as they avoid frequent account lockouts.

## Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

### Dictionary Attacks

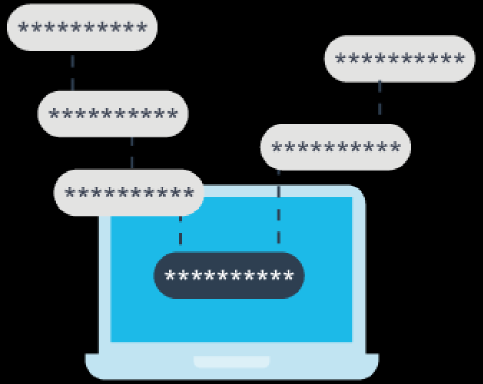
This technique attempts to gain access to a system by ‘spraying’ a few commonly used passwords across a large number of accounts. For example, a cybercriminal uses 'Password123' with many usernames before trying again with a second commonly-used password, such as ‘qwerty.’
This technique allows the perpetrator to remain undetected as they avoid frequent account lockouts.

Methods of Infiltration

## Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

### Brute-Force Attacks



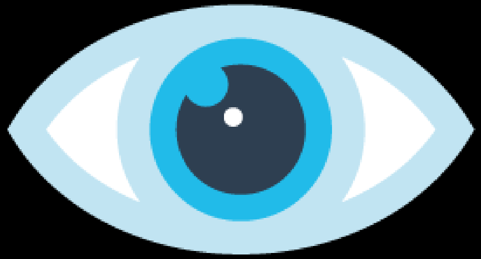
Plain text or unencrypted passwords can be easily read by other humans and machines by intercepting communications.
If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it.

# Methods of Infiltration

## Password Attacks

Entering a username and password is one of the most popular forms of authenticating to a web site. Therefore, uncovering your password is an easy way for cybercriminals to gain access to your most valuable information.

## Traffic Interception



Plain text or unencrypted passwords can be easily read by other humans and machines by intercepting communications.

If you store a password in clear, readable text, anyone who has access to your account or device, whether authorized or unauthorized, can read it.

## Cracking Times

It looks as if the hackers are trying everything to crack @Apollo's private Wi-Fi password. We have to make sure that the password is strong enough to withstand their attack!

Take a look at the following passwords. Put them in the correct order according to how long you think it would take an attacker to crack each one using brute-force, where 1 is the shortest amount of time and 4, the highest.

A. Password
B. 3trawberry
C. K4km9n2R
D. H$1gh#7iD@3

✓

## It’s Over to You...

Phew! That’s a lot to take in and hackers certainly have a lot of tools at their disposal. It is important that you know what these are so that you can protect yourself and @Apollo.
You think back to some of the suspicious activities that you’ve seen recently in the organization.
Based on what you have learned in this topic, what type of attack could each of these scenarios be?

**On your way into the office, a person whom you have never seen before asks you to hold the door — they forgot their access card**

A. **DoS**
B. **SEO poisoning**
C. **Social engineering**

## It’s Over to You...

Phew! That’s a lot to take in and hackers certainly have a lot of tools at their disposal. It is important that you know what these are so that you can protect yourself and @Apollo.
You think back to some of the suspicious activities that you’ve seen recently in the organization. Based on what you have learned in this topic, what type of attack could each of these scenarios be?

**You have started getting an error message when accessing your computer: ‘Your connection was interrupted. A network change was detected.’**

A. **DoS**
B. **SEO poisoning**
C. **Social engineering**

✓

## It’s Over to You...

Phew! That’s a lot to take in and hackers certainly have a lot of tools at their disposal. It is important that you know what these are so that you can protect yourself and @Apollo.
You think back to some of the suspicious activities that you’ve seen recently in the organization. Based on what you have learned in this topic, what type of attack could each of these scenarios be?

**You searched for @Apollo’s website on Google, but when you clicked on the top result, you were redirected to a page advertising antivirus software**

A. **DoS**
B. **SEO poisoning**
C. **Social engineering**

# Security Vulnerability and Exploits

# Security Vulnerability and Exploits

Before we get into the details, let’s start by outlining some key terms that you need to know.
***Security vulnerabilities*** are any kind of software or hardware defect.
A program written to take advantage of a known vulnerability is referred to as an ***exploit***.
A cybercriminal can use an exploit against a vulnerability to carry out an *attack*, the goal of which is to gain access to a system, the data it hosts or a specific resource.

# Hardware Vulnerabilities

***Hardware vulnerabilities*** are most often the result of hardware design flaws. For example, the type of memory called RAM basically consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors. Based on this design flaw, an exploit called Rowhammer was created. By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM.

# Hardware Vulnerabilities

***Hardware vulnerabilities*** are most often the result of hardware design flaws. For example, the type of memory called RAM basically consists of lots of capacitors (a component which can hold an electrical charge) installed very close to one another. However, it was soon discovered that, due to their close proximity, changes applied to one of these capacitors could influence neighbor capacitors. Based on this design flaw, an exploit called Rowhammer was created. By repeatedly accessing (hammering) a row of memory, the Rowhammer exploit triggers electrical interferences that eventually corrupt the data stored inside the RAM.

***Meltdown and Spectre***

Google security researchers discovered Meltdown and Spectre, two hardware vulnerabilities that affect almost all central processing units (CPUs) released since 1995 within desktops, laptops, servers, smartphones, smart devices and cloud services.

Attackers exploiting these vulnerabilities can read all memory from a given system (Meltdown), as well as data handled by other applications (Spectre). The Meltdown and Spectre vulnerability exploitations are referred to as side-channel attacks (information is gained from the implementation of a computer system). They have the ability to compromise large amounts of memory data because the attacks can be run multiple times on a system with very little possibility of a crash or other error.

# Hardware Vulnerabilities

***Meltdown and Spectre***

Google security researchers discovered Meltdown and Spectre, two hardware vulnerabilities that affect almost all central processing units (CPUs) released since 1995 within desktops, laptops, servers, smartphones, smart devices and cloud services. Attackers exploiting these vulnerabilities can read all memory from a given system (Meltdown), as well as data handled by other applications (Spectre). The Meltdown and Spectre vulnerability exploitations are referred to as side-channel attacks (information is gained from the implementation of a computer system). They have the ability to compromise large amounts of memory data because the attacks can be run multiple times on a system with very little possibility of a crash or other error.

Hardware vulnerabilities are specific to device models and are not generally exploited through random compromising attempts. While hardware exploits are more common in highly targeted attacks, traditional malware protection and good physical security are sufficient protection for the everyday user.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

**Buffer Overflow**

Buffers are memory areas allocated to an application. A vulnerability occurs when data is written beyond the limits of a buffer. By changing data beyond the boundaries of a buffer, the application can access memory allocated to other processes. This can lead to a system crash or data compromise, or provide escalation of privileges.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

## Non-Validated Input

Programs often require data input, but this incoming data could have malicious content, designed to force the program to behave in an unintended way.

For example, consider a program that receives an image for processing. A malicious user could craft an image file with invalid image dimensions. The maliciously crafted dimensions could force the program to allocate buffers of incorrect and unexpected sizes.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

## Race Conditions

This vulnerability describes a situation where the output of an event depends on ordered or timed outputs. A race condition becomes a source of vulnerability when the required ordered or timed events do not occur in the correct order or at the proper time.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

## Weaknesses in security practices

Systems and sensitive data can be protected through techniques such as authentication, authorization and encryption. Developers should stick to using security techniques and libraries that have already been created, tested and verified and should not attempt to create their own security algorithms. These will only likely introduce new vulnerabilities.

# Software Vulnerabilities

Software vulnerabilities are usually introduced by errors in the operating system or application code.

Most software security vulnerabilities fall into several main categories.

## Access control problems

Access control is the process of controlling who does what and ranges from managing physical access to equipment to dictating who has access to a resource, such as a file, and what they can do with it, such as read or change the file. Many security vulnerabilities are created by the improper use of access controls.

Nearly all access controls and security practices can be overcome if an attacker has physical access to target equipment. For example, no matter the permission settings on a file, a hacker can bypass the operating system and read the data directly off the disk. Therefore, to protect the machine and the data it contains, physical access must be restricted, and encryption techniques must be used to protect data from being

# Software Updates

The goal of software updates is to stay current and avoid exploitation of vulnerabilities. Microsoft, Apple and other operating system producers release patches and updates almost every day and applications such as web browsers, mobile apps and web servers are often updated by the companies or organizations responsible for them.

Despite the fact that organizations put a lot of effort into finding and patching software vulnerabilities, new vulnerabilities are discovered regularly. That’s why some organizations use third party security researchers who specialize in finding vulnerabilities in software, or actually invest in their own penetration testing teams dedicated to search, find and patch software vulnerabilities before they can get exploited.

Google’s Project Zero is a great example of this practice. After discovering a number of vulnerabilities in various software used by end users, Google formed a permanent team dedicated to finding software vulnerabilities.

# What Do You Think?

This has made you think about some of the vulnerabilities that may exist at @Apollo.
After some investigation you’ve noted some potential issues.
***Can you identify what category each of these vulnerabilities falls into?***

# What Do You Think?

This has made you think about some of the vulnerabilities that may exist at @Apollo. After some investigation you've noted some potential issues.
***Can you identify what category each of these vulnerabilities falls into?***

On starting at @Apollo, your network password was emailed to you in plain text and you were not prompted to change it

A. Weakness in security practice
B. Access control problem
C. Non-validated input

# What Do You Think?

This has made you think about some of the vulnerabilities that may exist at @Apollo. After some investigation you've noted some potential issues.
***Can you identify what category each of these vulnerabilities falls into?***

Past employees still have access to @Apollo's customer database

A. Weakness in security practice
B. Access control problem
C. Non-validated input

## What Do You Think?

✓

This has made you think about some of the vulnerabilities that may exist at @Apollo. After some investigation you’ve noted some potential issues.

***Can you identify what category each of these vulnerabilities falls into?***

New users can log into their @Apollo account, even if they have signed up with an incorrectly formatted email address

A. Weakness in security practice
B. Access control problem
C. Non-validated input

# The Cybersecurity Landscape

# The cybersecurity Lanscape

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

The cybersecurity Lanscape

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

Cryptocurrency owners keep their money in encrypted, virtual ‘wallets.’ When a transaction takes place between the owners of two digital wallets, the details are recorded in a decentralized, electronic ledger or blockchain system. This means it is carried out with a degree of anonymity and is self-managed, with no interference from third parties such as central banks or government entities.

The cybersecurity Lanscape

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

Approximately every ten minutes, special computers collect data about the latest cryptocurrency transactions, turning them into mathematical puzzles to maintain confidentiality.

These transactions are then verified through a technical and highly complex process known as ‘mining.’ This step typically involves an army of ‘miners’ working on high-end PCs to solve mathematical puzzles and authenticate transactions.

# The cybersecurity Lanscape

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

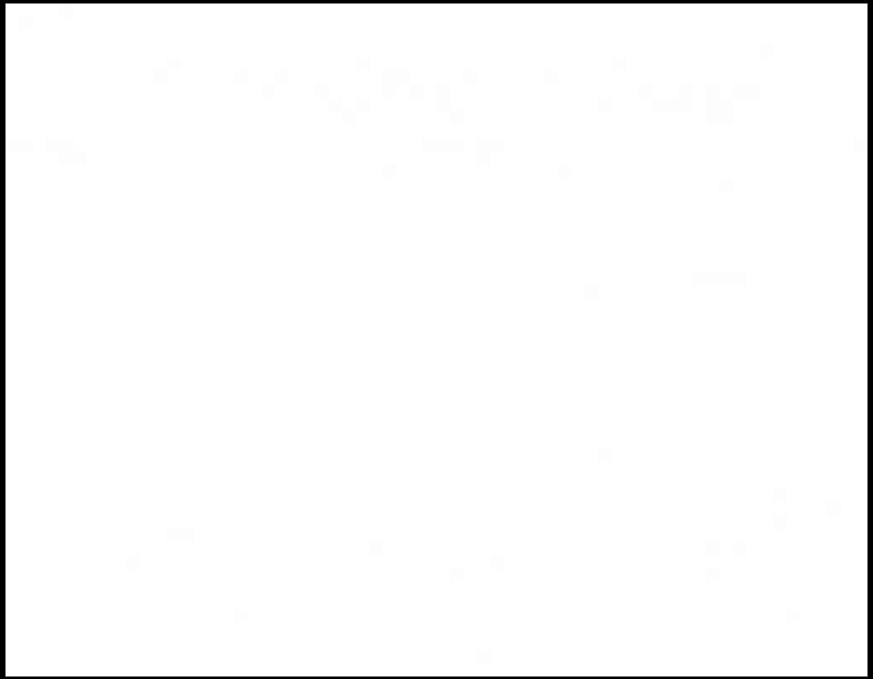
# The cybersecurity Lanscape

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?

Once verified, the ledger is updated and electronically copied and disseminated worldwide to anyone belonging to the blockchain network, effectively completing a transaction.

# Cryptojacking

You’ve likely heard of cryptocurrency, but do you know exactly what it is and how it works?



Cryptojacking is an emerging threat that hides on a user’s computer, mobile phone, tablet, laptop or server, using that machine’s resources to 'mine’ cryptocurrencies without the user's consent or knowledge.

Many victims of cryptojacking didn’t even know they’d been hacked until it was too late!

Quiz

# Protecting Your Devices and Network

# Protecting Your Devices and Network

You’ve probably heard of the term ‘online security.’ It’s all about taking the necessary steps to prevent your personal information from falling into the wrong hands.

# Protecting Your Computing Devices

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it’s important to protect the security of your devices.

**Turn on the Firewall**

You should use at least one type of firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access. The firewall should be turned on and constantly updated to prevent hackers from accessing your personal or organization data.

# Protecting Your Computing Devices

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it’s important to protect the security of your devices.

## Turn on the Firewall

You should use at least one type of firewall (either a software firewall or a hardware firewall on a router) to protect your device from unauthorized access. The firewall should be turned on and constantly updated to prevent hackers from accessing your personal or organization data.

## Install Antivirus and Antispyware

Malicious software, such as viruses and spyware, are designed to gain unauthorized access to your computer and your data. Once installed, viruses can destroy your data and slow down your computer. They can even take over your computer and broadcast spam emails using your account. Spyware can monitor your online activities, collect your personal information or produce unwanted pop-up ads on your web browser while you are online.

To prevent this, you should only ever download software from trusted websites. However, you should always use antivirus software to provide another layer of protection. This software, which often includes antispyware, is designed to scan your computer and incoming email for viruses and delete them. Keeping your software up to date will protect your computer from any new malicious software that emerges.

# Protecting Your Computing Devices

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it’s important to protect the security of your devices.

**Manage Your Operating System and Browser**

Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari).

Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer’s operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

# Protecting Your Computing Devices

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it’s important to protect the security of your devices.

## Manage Your Operating System and Browser

Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari).

Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer’s operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

## Set up Password Protection

All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access. Any stored information, especially sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost.

Remember, if any one of your devices is compromised, the criminals may be able to access all of your data through your cloud storage service provider, such as iCloud or Google Drive.

# Protecting Your Computing Devices

Your computing devices are the portal to your online life, storing a lot of your personal data. Therefore, it’s important to protect the security of your devices.

## Manage Your Operating System and Browser

Hackers are always trying to take advantage of vulnerabilities that may exist in your operating system (such as Microsoft Windows or macOS) or web browser (such as Google Chrome or Apple Safari).

Therefore, to protect your computer and your data, you should set the security settings on your computer and browser to medium level or higher. You should also regularly update your computer’s operating system, including your web browser, and download and install the latest software patches and security updates from the vendors.

## Set up Password Protection

All of your computing devices, including PCs, laptops, tablets and smartphones, should be password protected to prevent unauthorized access. Any stored information, especially sensitive or confidential data, should be encrypted. You should only store necessary information on your mobile device, in case it is stolen or lost.

Remember, if any one of your devices is compromised, the criminals may be able to access all of your data through your cloud storage service provider, such as iCloud or Google Drive.