UNITED ARAB EMIRATES
MINISTRY OF EDUCATION

Cyber Security

Cycle 3 – Grade 12

Chapter 1
Security

Chapter overview

In this chapter, you will learn about security in computing systems and networks. You will learn about cyber attacks and the different types of cyber attacks. You will also study the different ways to prevent cyber attacks. You will be able to differentiate between active and passive attacks. You will also learn the different types of malicious attacks on a network. You will be introduced to ethical hacking and the CIA triad in security. Finally, you will learn ethics and data privacy in cyber security.

This chapter is organised as follows. Section 1 will introduce you to cyber security and the different types of cyber attacks, including active and passive. You will learn what is ethical hacking and what are the security threats in mobile environments. Section 2 focuses on cyber safety and how to prevent cyber attacks. You will study the CIA triad and its significance in security. Section 3 will introduce you to cyber security ethics and data privacy in networks.

Section 1 : Network security and types of attacks

Aim

This section will introduce cyber attacks and different types of cyber attacks. This will be followed by discussing the different stages in the lifecycle of ethical hacking. You will learn about the different types of malicious software. You will also learn about passive and active attacks and how to distinguish between them. Finally, you will learn about the various types of mobile security threats.

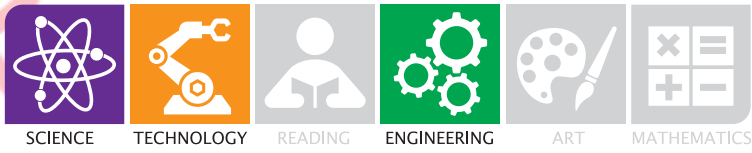
Learning outcomes

- Show the different types of cyber attacks.
- Illustrate the lifecycle of ethical hacking.
- Compare types of malicious software.
- Differentiate between passive and active attacks.
- Categorise mobile security threats.

Prior knowledge

- Computer Science
- Networking

My STREAM Focus



Key vocabulary

WORD	MEANING	PICTURE
cyber security	practice of protecting systems, networks, and programs from digital attacks	
cyber attack	harmful and purposeful attempt by an individual or organisation to enter another person's or organisation's information system	
ethical hacking	hackers who are legally permitted to break into certain computer systems to find flaws	
malicious software	also called malware, is an intrusive software that is designed to damage and destroy computers and computer systems	

Cyber security

Information or data produced or stored by electronic or digital means are called **electronic** or **digital information**. Electronic information is connected as a network and has become an integral part of humans' daily lives. All types of organisations like educational institutions, hospitals and financial companies use this network to operate effectively by collecting, processing, storing, and sharing digital information. As more digital information is collected and exchanged, the security of this data becomes increasingly important for national security and economic stability.

The levels of data protection are as follows:

- Personal level
- Organisation level
- Government level

Figure 1.1.1

Cyber security is a process to protect individuals, organisations, and governments from digital attacks. In this process the networked systems and data are protected from attackers. **Cybercriminals** are individuals or groups of individuals who use technology to commit destructive, illegal activities. These activities are referred to as **cyber attacks**, and they are performed on digital systems or networks with the intention to disable computers and steal sensitive data. Cybercriminals can also use a breached computer system to start additional attacks and damages at the personal, organisational, or governmental level. Any criminal activity that involves a computer, networked device or a network is called **cybercrime**. A **cyber threat** is a successful cyber attack that can come from within an organisation by trusted users or from remote locations by unknown parties. Threats are always present and can be purposeful or undirected. For example, hackers purposefully threaten unprotected information systems in an organisation. **Vulnerability** is a weakness or fault in a system or protection mechanism that opens it to attack or damage—for example, a flaw in a software package or an unprotected system port. Consider an unlocked door at home. If the door is unlocked or has a broken lock, that certainly compromise the security of everything inside the room. Issues like these increase the risk of a system.

HB **Complete activities 1.1.1 and 1.1.2 in your workbook.**

Types of attackers

Individuals or groups who attempt to exploit the vulnerability for personal or financial advantage are known as **attackers**. Credit cards, product designs, and anything else of value are targets for attackers. Attacks can be originated from within (internal) an organisation or from outside (external) of the organisation.

Internal threats

An employee or company's partner can:
- mishandle confidential data
- disrupt internal server / network operations
- use infected USB to facilitate outside attacker to enter the organization
- open attackers emails/links accidentally and infect the network or computer systems

External threats

Amateurs or skilled attackers can:
- exploit vulnerabilities in network or computer systems through attackers
- use gain access to the network or computer systems through attacker's different skills

Figure 1.1.2

Attackers are categorised as:
- Amateurs
- Hackers
- Organised hackers

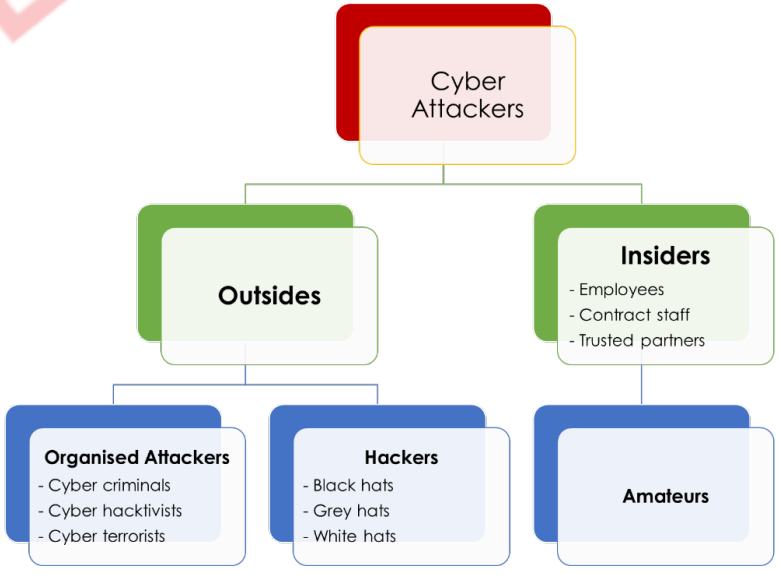


Figure 1.1.3 : Different cyber attackers

Amateurs

Figure 1.1.4 : Amateur attacker

Script Kiddies is a term used to describe **amateur attackers**. They are mainly inexperienced attackers who start attacks using pre-existing tools or instructions obtained on the internet. Few attackers are simply interested, while others are attempting to demonstrate their abilities by causing harm. Even if they are employing simple instruments, the impact can be severe to any computing system.

Hackers

This group of attackers break into computers or networks to gain access. Depending on the intent of the break-in, these attackers are classified as:

- White hat hackers
- Grey hat hackers
- Black hat hackers

Figure 1.1.5 : Black, Grey and White hat hackers

White hat hackers

An **ethical hacker** is an information security expert who enters a computer system, network, application, or other computing resources with its owner's permission. A **white hat hacker** is also known as an ethical hacker or a computer security expert who never intends to harm a system and has a code of ethics. The white hat attackers discover the weaknesses in a network or computer systems so that the security of these systems can be improved.

Black hat hackers

A **black hat hacker** is also known as a cracker or illegal hacker. Their act operates on the opposite side of the law. Personal or financial gain is frequently the key motivation to black hat hackers. They hack to obtain unauthorised access to a system, disrupt its operations, or steal sensitive data, violating people's privacy, causing system damage, and blocking network communication. Without contacting the victim, a black hat hacker may disclose the exploit to other hackers and/or the public. This allows others to take advantage of the vulnerability before the organisation can fix it.

Grey hat hackers

A **grey hat hacker** is a computer hacker or computer security expert who combines the skills of both black and white hat hackers. They may break laws or ethical standards to take advantage of a security flaw in a computer system or network without the owner's permission or knowledge. Their goal is to bring the flaw to the owners' attention to gain appreciation or compensation from them. Some grey hat hackers post information about the vulnerability on the internet so that other attackers might take advantage of it.

Organised hackers

Cybercriminals are organised cybercriminals, hacktivists, cyber terrorists, and state-sponsored hackers. Cybercriminals are groups of professional criminals seeking power, money, and control. The criminals are well-organised and sophisticated, and they may even offer cybercrime as a service to other criminals. Hacktivists make political comments to raise awareness about problems that are important to them. On behalf of their government, the attackers acquire intelligence to damage. These attackers are typically well-trained and well-funded, and their attacks are targeted towards specific objectives that benefit their government.

Figure 1.1.6 : Cybercrime

HB **Complete activities 1.1.3 and 1.1.4 in your workbook.**

What is an attack vector?

An **attack** is an intentional act that exploits the vulnerability and can be a direct or indirect attack. Examples of attacks include destruction, modification, fabrication, interruption, or interception of data.

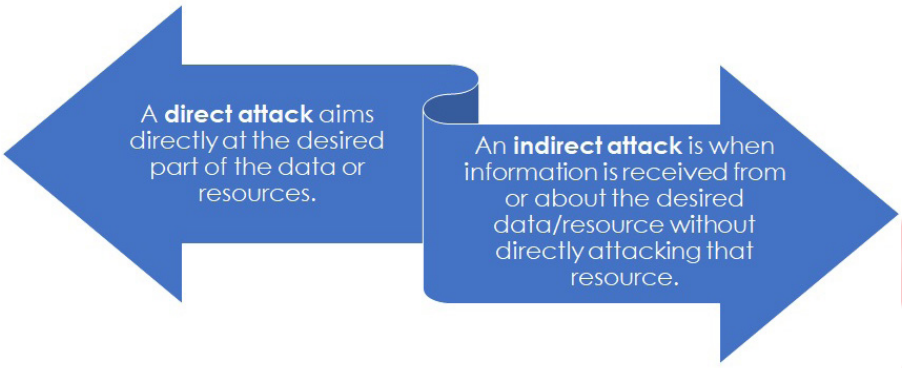


Figure 1.1.7 : Direct and indirect attack

An **attack vector** is a path, technique, or mechanism by which someone gains illegal (unauthorised) access to a computer or network server to deliver a virus payload or malicious entry into a system.

It enables hackers to exploit system vulnerabilities, including the human element, and often includes using email to deliver the malware. Examples of attack vector methods are the use of email attachments to send malware spam and bogus links, which lead to cybersecurity breaches. These can be prevented by educating employees on how to avoid clicking suspect links that could lead to a phishing attack or making sure all the company's systems are robust enough to prevent these common types of attacks.

Figure 1.1.8

Table 1.1.1

Vector	Description
IP scan and attack	The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox.
web browsing	If the infected system has write access to any webpages, it makes all web content files (.html, .asp, .cgi and others) infectious so that users who browse to those pages become infected.
virus	Each infected machine infects certain common executable or script files on all computers, which it can write with virus code that can cause infection.
unprotected shares	Using vulnerabilities in file systems and the way many organisations configure them, the infected machine copies the viral component to all locations it can reach.

mass mail	By sending email infections to addresses found in the address book. The infected machine infects many users whose mail-reading programs automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	By using widely known and common passwords that were employed in early versions of this protocol (which is used for remote management of network and computer devices), the attacking program can gain control of the device. Most vendors' attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Types of cyber attacks

Cybersecurity is the process of defending networks and computing systems against cyber attacks that aim to gain access to, alter, or destroy sensitive data. People face the risk of being extorted money or having their usual business processes disrupted. No one can afford to overlook the importance of cybersecurity in today's technological environment. Electronic devices, phones, and everything that may be connected to a computer or the internet are subject to cyber attacks by cybercriminals. As a result, it is critical that you understand the several types of cyber threats.

The following are some of the threats that exist today:
- Malware
- Social engineering
- Denial-of-service
- Wi-Fi password cracking

Malwares

Malware is software written to harm or cause issues with a computer. It is also called **malicious** code or **malicious software**. This code comes in several forms and either harms or steals data from a computer system. Cybercriminals use many different types of malwares or malicious software to carry out their activities.

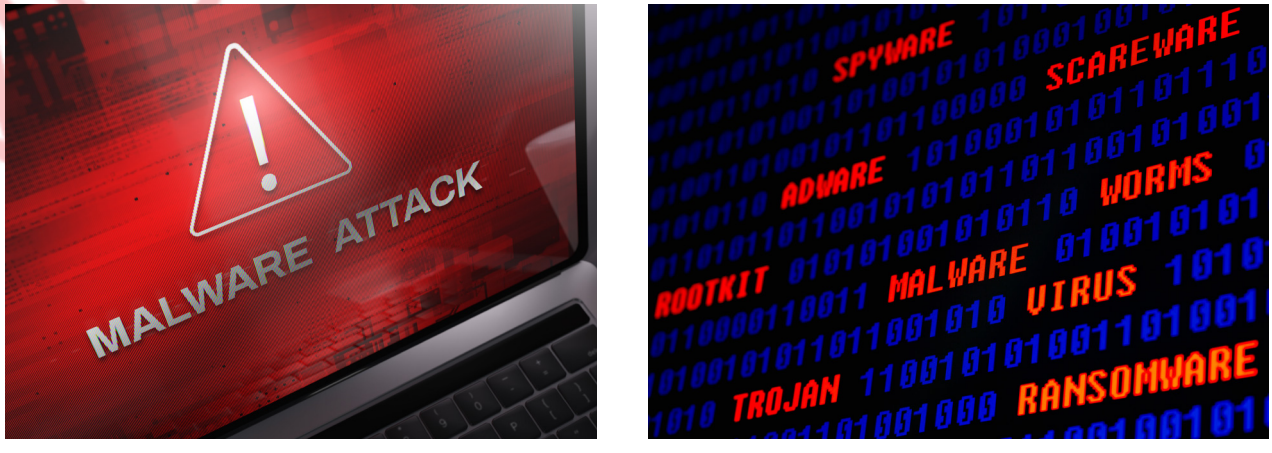


Figure 1.1.9 : Malware attacks

Signs of malware attack in a system

You can identify the signs and symptoms of a malware attack as the attacks are obvious or discrete. Here are a few common signs that may indicate you have a malware infection.

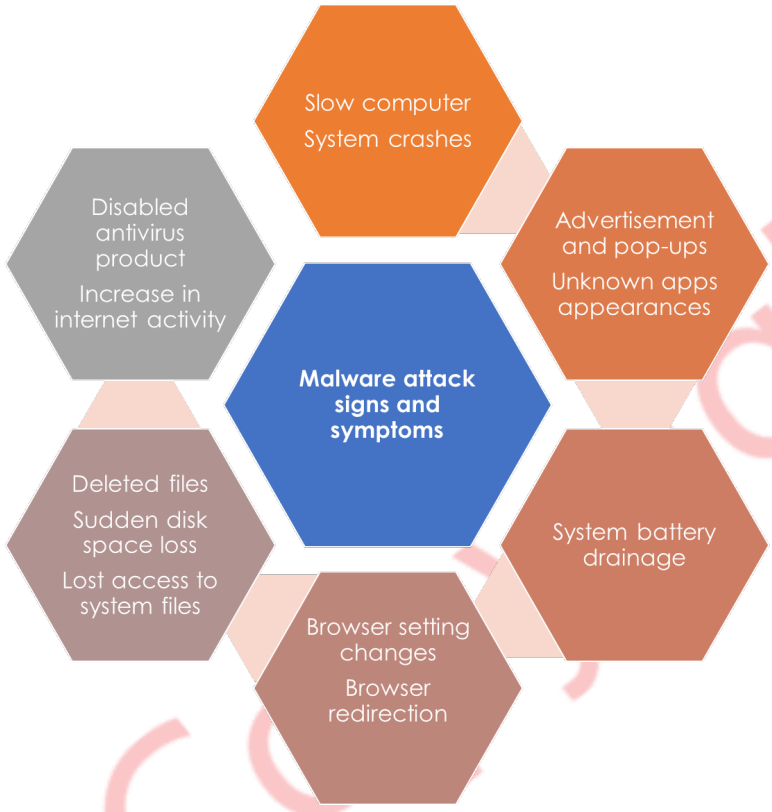


Figure 1.1.10 : Signs of malware attack

Types of malwares

Spyware

Spyware is a type of malware that is designed to track and spy on a computer system. It secretly collects the activity on a computer system and then sends the collected data to another person without the awareness of the computer system owner.

Figure 1.1.11

A computer gets infected by spyware by modifying the security settings of a device. A spyware can:

- monitor online activities.
- log every key pressed on a keyboard as a keylogger.
- capture all the personal data like passwords or bank details.

A spyware can join itself with legitimate software or Trojan horses. Anti-spyware software is available to detect and remove unwanted spyware programs.

Example:

CoolWebSearch – This spyware attacks the web browser, changes the settings, and sends the browsing data to the author who created this spyware.

Gator – This spyware monitors the victim's web surfing habits and uses the information to serve them with specific advertisements.

Virus

A virus is a type of malware that infects a computer when executed and then replicates itself to pass to another computer. Most viruses are spread by USB drives, optical disks, network shares or email.

Figure 1.1.12 : Virus

Example:
Melissa - This virus was spread by email, using a malicious attachment and infected thousands of computers worldwide by the end of 1999. Reports from that time say that it infected many companies, causing losses estimated at USD 80 million.

Trojan horse

This malware is named after the Greek myth of the Trojan horse. Trojans exploits user privileges and are often found in image files, audio files or games. Unlike viruses, Trojans do not self-replicate but carry out malicious operations by hiding their purpose. Trojans appears genuine, but it is very dangerous. Anti-virus software is available to remove the trojans.

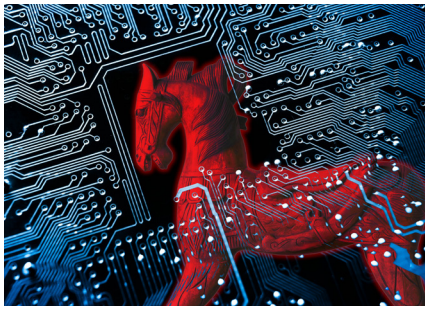


Figure 1.1.13 : Trojan

Example:
Qbot - This has been a banking trojan active since 2007. It is focused on stealing user data and banking credentials.

TrickBot – This is a trojan developed and operated by attackers in 2016. This trojan is a banking trojan that steals financial data. Later the trojan evolved with additional features that provide its operators with a full suite of tools to carry out numerous illegal cyber activities.

Worms

This malware replicates itself to spread from one computer to another. Initially, the host is infected. After that, the worm does not require any user's participation. It can run by itself and can spread very quickly over the network. Worms can exploit the system vulnerabilities and can move themselves to cause damage to computer systems or networks. Installing good anti-virus software can protect the computer systems or networks from getting infected with worms.

Figure 1.1.14 : Worm

Example:
SQL Slammer – In 2003, this program generated random IP

addresses, looking for those not protected by anti-virus software. The infected systems were more than 75,000 that unknowingly involved in DDoS distributed denial-of-service (DDoS) attacks on several major websites. In the years 2016 and 2017, this worm again revived. Through relevant security patches, this worm can be avoided from infecting the systems. You will learn about DDoS attacks later in the chapter.

Adware

Adware is a type of malware that is installed with some versions of software and is designed to automatically deliver advertisements to a user on a web browser. It causes pop-up ads on the screen that are sometimes difficult to close. It is common for adware to come with spyware. Anti-virus or anti-adware software are available to detect and prevent adware from infecting a computer system.

Figure 1.1.15 : Adware

Example:
Fireball – This adware program when affects the computer, it takes over your browser, changes the homepage to a fake search engine called Trotus. Then it inserts obtrusive ads into any webpage a user visits and prevents them from modifying the browser settings.

Appearch – This adware is a browser hijacker. It is usually bundled with other free software, and it inserts many ads into the browser. This makes web browsing difficult and redirects the user to Appreach.info instead. When a web page is tried to open, Appearch adware program converts random blocks of text into links in that web page. Therefore, when the text is selected, a pop-up invites the to download software updates.

Ransomware

Ransomware is a type of malware that hijacks the data on a computer system by encrypting it and then demands the owners to pay money for the data to be decrypted. Ransomware is often spread through phishing emails that encourage users to download a malicious attachment. Anti-virus software is available to prevent the computer system from ransomware attacks.

Figure 1.1.16 : Randomware

Example:
CryptoLocker - In 2013 and 2014, cybercriminals used social engineering technique (to be explained later in the chapter), to convince employees and download this ransomware to their computers. When ransomware is downloaded, this program then infects the networks. CryptoLocker would display a ransom notice offering to decode the data if a cash or Bitcoin payment was made by the specified time. It is thought that the program's creators extorted roughly three million dollars from businesses.

Backdoor

A backdoor malware works in the background of a computer system and is difficult to detect. Backdoor malware gains unauthorised access to a system by bypassing the normal authentication procedures. After the backdoor attack, the hackers can remotely access the resources through system commands.

Figure 1.1.17 : Backdoor

Example:
PoisonTap - This backdoor malware allows hackers to access almost any website that a user has logged in to. For example, this program can be installed by directly plugging a microcontroller/ microprocessor into the USB port.

Scareware

Scareware is a type of malware that uses 'scare' tactics to take a specific action. Scareware usually consists of operating system style windows that pop up to warn the user that the system is at risk and needs to run a specific program for it to return to normal operation. If the user gets scared and accepts to execute that specific program, then the computer system will become infected with scareware malware.

Figure 1.1.18 : Scareware

Example:
In 2006, Microsoft users got affected by scareware. An online payment processor, known as ChronoPay, approached Mac users in 2009 with scareware that made the users buy fake anti-virus software. In 2010, newspaper readers were attracted by advertisements that led them to fake websites and downloaded malware on their devices.

Rootkit

Rootkit malware is like backdoor malware and is designed to modify the operating system. Rootkit malware are hard to detect as the attackers gain access to resources remotely to modify the system files, system investigating file and monitoring tools. Therefore, a computer infected with rootkit malware is completely wiped, and new software gets installed.

Example:
In 2020, Spicy Hot Pot, a browser hijacking rootkit, attacked many systems. This program changes a user's homepage to point to a page controlled by the malware operator. Along with this, the program uploads memory dumps to the user from a machine to a predefined server with a local update feature to ensure it can remain updated.

Figure 1.1.19 : Rootkit

Malware prevention

The following methods are a few ways to prevent a system from malware attacks.

- Use strong passwords
- Do not lend your device to others and stay cautious when online
- Educate yourself about malwares and prevention methods
- Download apps from official app stores
- Be aware of all email attachments
- Use virtual private networks (VPNs)
- Keep all system software updated

Figure 1.1.20

Social engineering

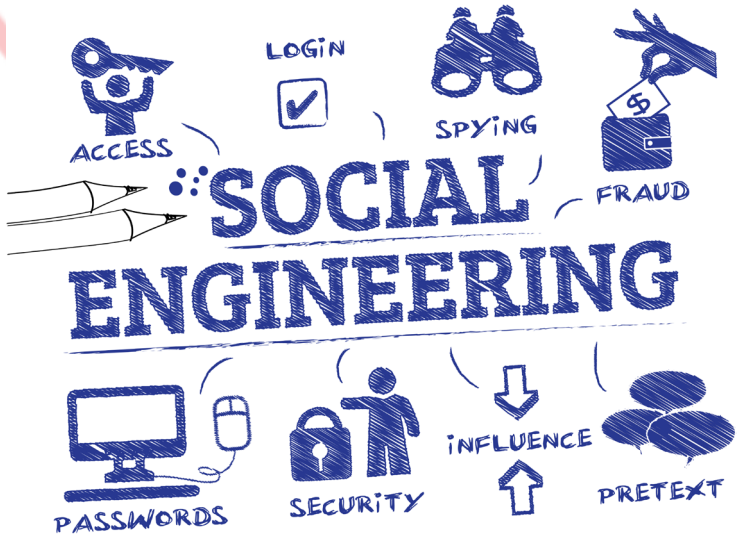


Figure 1.1.21 : Social engineering

Social engineering is a kind of cyberattack that involves psychological manipulation technique that exploits human error to access confidential information. It is like a trick to gain people's confidence, to gather information and gain unauthorised access to the computer system.

For example, an attacker will call an authorised employee with an urgent problem that requires immediate network access. The attacker will try using techniques to gain the trust of the employee to access confidential data.

Figure 1.1.22 : Hacking through social engineering

Phishing is a common social engineering attack. The attackers contact a target through email, phone, or text message to click a link. This link will redirect the targets to fraudulent websites to provide confidential data like personal information, banking and credit card information, usernames, and passwords.

Figure 1.1.23 : Phishing

Denial-of-Service

Figure 1.1.24 : Denial -of-Service attack

Denial-of-Service (DoS) attacks are a type of network attack that results in some sort of interruption of network service to users, devices, or applications.

An overwhelming quantity of traffic is a type of DoS attack in a network where an enormous amount of data is sent to the host at a rate that it cannot handle. This kind of attack causes a slowdown in transmission or response, or the device or service to crash.

A maliciously formatted packet is a type of DoS attack. When a maliciously formatted packet (collection of data) is sent, the receiver cannot identify the application and will be unable to handle it. As a result of this, the system will run very slowly.

Distributed DoS

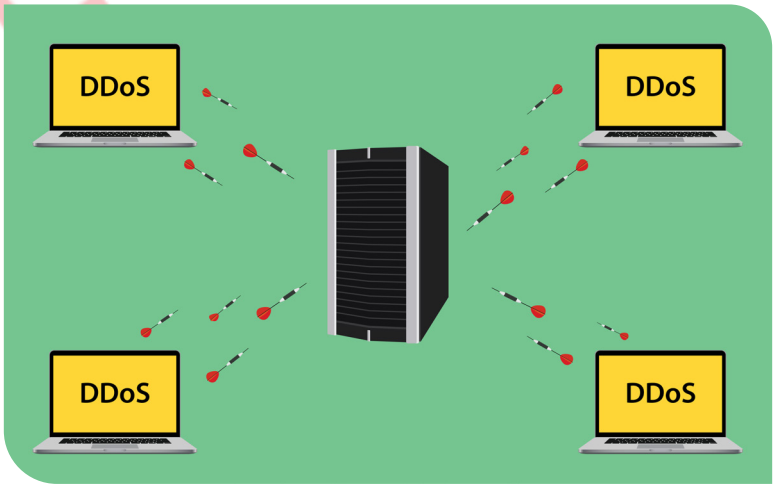


Figure 1.1.25 : Distributed DoS

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 needed, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

Botnet

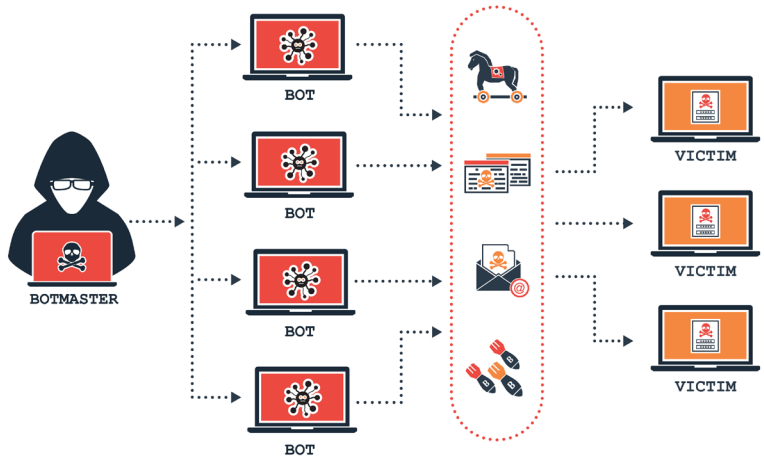


Figure 1.1.26 : Botnet

A **bot computer** is typically infected by visiting an unsafe website or opening an infected email attachment or media file. A botnet is a group of bots where hundreds of thousands of bots are connected through the internet. A botnet is controlled by cyber attackers through system commands.

On-path attacks

On-path attack is also referred to as a **man-in-the-middle (MitM)** or **man-in-the-mobile (MitMo)** attack. This attack intercepts or modifies communications between two devices, such as a web browser and a web server, to collect information from the devices.

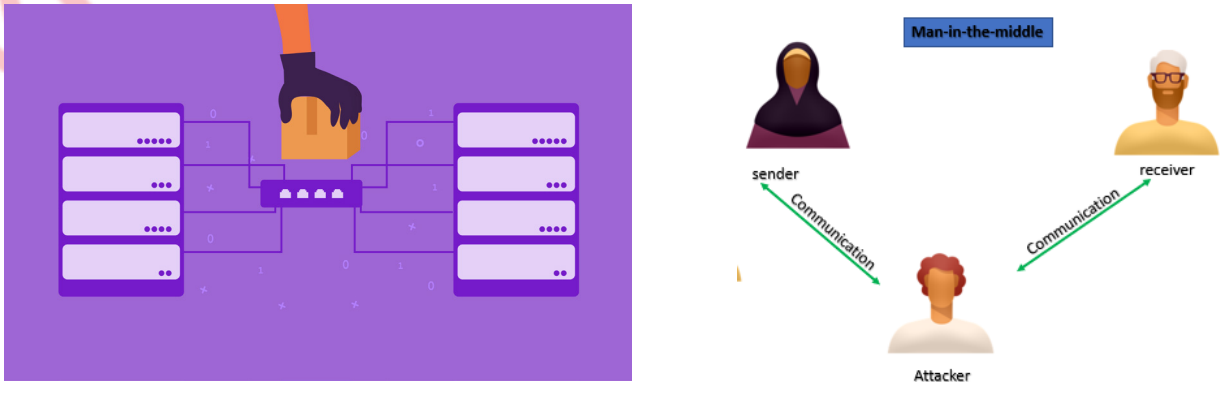


Figure 1.1.27 : Man-in-middle attack

A **MitM attack** happens when a cybercriminal takes control of a device and captures users' information without the user's knowledge. These types of attacks are often used to steal financial information.

A **MitMo** is a type of attack used to take control over a user's mobile device. When the mobile device is infected, the confidential data is captured and sent to the attackers.

Figure 1.1.28 : Man-in-the-mobile attack

SEO poisoning

After a search using search engines like Google, the web pages are rank wise listed according to the relevancy of their content. Attackers use popular search terms and use SEO to push malicious sites to higher up the ranks of search results. This technique is called **Search Engine Optimisation (SEO) poisoning.**

Wi-Fi password cracking

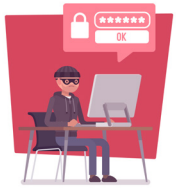
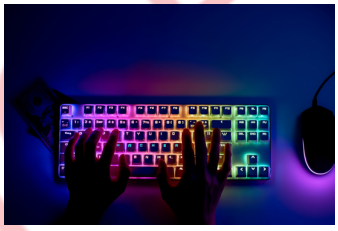
Password attacks

One of the most common methods of authenticating a website is by entering a username and password. As a result, revealing your password is a simple way for cybercriminals to gain access to your most sensitive information.

Figure 1.1.29 : Password cracking

The table below describes the different kinds of password attacks.

Table 1.1.2

Password attack	Description
Password spraying 	This method tries to gain access to a system by 'spraying' a few commonly used passwords across many accounts. For example, a cybercriminal may use 'Password123' with a variety of usernames before attempting a second commonly used password, such as 'qwerty.'
Dictionary attacks 	In an attempt to gain access to a password-protected account, a hacker systematically tries every word in a dictionary or a list of commonly used words as a password.
Brute-force attacks 	Brute-force attacks are the most basic and widely used method of gaining access to a password-protected site. They involve an attacker trying every possible combination of letters, numbers, and symbols in the password space until they get it right.
Rainbow attacks 	In a computer system, passwords are stored as numerical values that uniquely identify data rather than plain text. A rainbow table is a large dictionary of precomputed values and the passwords that were used to generate them.
Traffic interception 	By intercepting communications, other humans and machines can easily read plain text or unsecured passwords. Anyone who has access to your account or device, whether authorised or unauthorised, can read your password if you store it in plain text.

HB **Complete activities 1.1.5 and 1.1.7 in your workbook.**

Passive and active attacks

Passive and active attacks are the two forms of attacks that are connected to security. An attacker tries to change the content of the messages in an active attack. An attacker observes the messages and copies them in a passive attack.

Passive attack

The passive attack is the first type of attack. For specific functions, a passive attack can monitor, observe, or develop use of the system's data. However, it has no effect on the system's resources, and the data remains unaffected. Because passive attacks are carried out in secret, it is difficult for the victim to notice them. The goal of a passive attack is to obtain data or to search the network for open ports and vulnerabilities.

Example:

Figure 1.1.30 : Eavesdropping

An eavesdropping attack is considered a type of passive attack. The goal of an eavesdropping attack is to steal data sent between two devices connected to the internet. Eavesdropping includes traffic analysis. An eavesdropping attack occurs when attackers introduce a software package into the network path in order to record future network traffic for research purposes. To collect network traffic, attackers must be forced to enter the network path between the endpoint and the communicationsystem. It will be easier for the attacker to put a software package into the network path if there are additional network methods and the network methods are lengthier.

Another type of passive attack is the distribution of messages. The attackers use a virus or malware to install a package on the device that allows them to monitor the device's operations, such as text messages, emails, or any transmitted files that include personal information and knowledge. The data will be used by the attackers to gain access to the device or network.

Active attacks

An active attack could be a network exploit in which the attackers modify or alter the content and cause a system resource to be affected. The victims will suffer harm because of it. The attackers can use passive attacks to gather information before launching a more forceful attack. The attackers try to break into the system and force it to lock. The victims can be alerted about

the active attack. Their integrity and accessibility may be threatened because of such an attack. A forceful attack is more difficult to execute than a passive attack.

Example:
One of the active attack samples is a denial-of-service assault (DoS). When attackers take action to shut down a tool or network, they are executing a denial-of-service attack. The first user may be unable to access the device or network because of this. The attackers can send a flood of traffic to the target device or network until it stops responding or flaming. Emails, websites, and online banking accounts are among the services that are affected. DoS assaults can be launched from virtually any location. DoS attacks include flooding or flaming the device and network.

One of the most popular DoS attacks is a buffer overflow. This type of flooding assault sends a large amount of traffic to the network, much exceeding the capacity of a buffer. The system will then be engulfed in flames. Furthermore, an Internet Control Message Protocol ICMP flood, often known as a ping flood, is a type of flooding attack. Spoofed packets and ICMP echo queries can be sent by the attacker. The network is compelled to respond to all claims. As a result, regular traffic may not be able to access the device.

What is a threat?

A **threat** is a possible object, person, or other entity that represents a constant danger to an asset. It can be seen as a potential violation of security that exists because of vulnerabilities. System controls let trespassers know they are invading on an organisation's cyberspace, but hackers use skill, guile, or fraud to bypass the controls protecting other people's information.

The main threat categories are:

1- Human threats – are acts of human failure or error, including acts done without malicious intent and caused by human inexperience, improper training or incorrect assumptions. For example, employees are amongst the greatest threats to any organisation for the following reasons, whcih can be prevented with appropriate controls:

- Employee mistakes can easily lead to the disclosure of classified data.
- Employees may enter erroneous data.
- Employees may accidentally delete or modify data.
- Employees may store data in unprotected areas or fail to protect information.

2- Deliberate acts of spying or trespass - access of protected information by unauthorised individuals.

3- Deliberate acts of theft - illegally taking another person's physical, electronic, or intellectual property. For example, shoulder surfing, occurs in any place a person accesses othersconfidential

information. In **shoulder surfing**, nformation such as personal identification numbers (PINs), passwords and other confidential data is obtained by looking over the victim's shoulder. Physical theft is controlled relatively easily, while electronic theft is a more complex problem as the evidence of the crime is not always apparent.

4- Deliberate software attacks - using malicious software (malware) designed to damage, destroy, or deny service to target systems. This includes viruses, worms, Trojan horses, back doors, and denial-of-service attacks.

5- Forces of nature - are among the most dangerous threats because they cause disruption not only to individual lives but also to the storage, transmission, and use of information. Organisations must implement controls to limit possible damage and prepare contingency plans for continued operations.

6- Deviations in quality of service - includes situations where products or services are not delivered as expected. Information systems depend on many interdependent support systems, internet service and communications. Power irregularities dramatically affect the availability of information and systems.

7- Internet service issues - Internet Service Provider (ISP) failures can considerably undermine the availability of information. Outsourced web hosting providers assume responsibility for all internet services as well as hardware and website operating system software.

Table 1.1.3

Categories of Threat	Examples
Acts of human error or failure	A person's mistake
Compromises to intellectual property	Piracy, copy infringement
Deliberate acts of espionage or trespass	Unauthorised access and/or data collection
Deliberate acts of information extortion	Blackmail of information discloser
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate acts of sabotage or vandalism	Deliberate acts of sabotage or vandalism
Deliberate software attacks	Viruses, worms, macros, denial-of-service
Forces of nature	Fire, flood, earthquake, lightning
Deviations in quality of service for service providers	Power and WAN issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Mobile security threats

Mobile security threats are attacks on mobile devices such as smartphones and tablets that aim to compromise or steal data. Malware or spyware are frequently used to give bad actors unauthorised access to a device. In many situations, consumers are unaware that an attack has happened.

With access, attackers can carry out a wide range of harmful activities, including stealing and selling data, gaining access to contacts, sending messages, and making phone calls. They can also utilise the gadget to steal login credentials and mimic other people. Individual users and organizations are also affected by these attacks, as a single breach could result in large-scale data releases.

Types of mobile threats

Attacks on mobile devices come in different shapes and sizes, but they generally fall into one of four categories, as listed below.

Mobile application security threats

When people download apps that appear to be trustworthy but actually steal data from their device, this is known as an application-based threat. Spyware and malware, for example, steal personal and business information without the user's knowledge.

Web-based mobile security threats

Web-based threats are mild and go undiscovered most of the time. They occur when users browse malicious websites. These websites will appear to be functioning normal on the surface but automatically will download malicious contents to the devices.

Mobile network security threats

Network-based threats are very common and risky now. Cybercriminals can steal unencrypted data when individuals use public Wi-Fi networks, making network-based risks more widespread and dangerous.

Mobile device security threats

Theft or loss of a device is the most common physical threats to mobile devices. This threat is especially dangerous for businesses because hackers have direct access to the hardware where confidential data is stored.

Ethical hacking

CLICK HERE

Figure 1.1.31 : Ethical hacking

Ethical hacking is the process of a professional hacker attempting to break into an organisation's computers and devices in a legal and intentional manner. Ethical hackers then put the organisation's defences to the test, exposing any weaknesses in their systems and networks. Finally, they submit a report outlining the organisation's overall risk and vulnerabilities, as well as ideas for improvement.

Types of ethical hacking

There are different kinds of ethical hacking practices. Every component of a system can be hacked and analysed. Hacking experts require deep knowledge regarding the component when hacking. A few common ethical hacking practices are listed below.

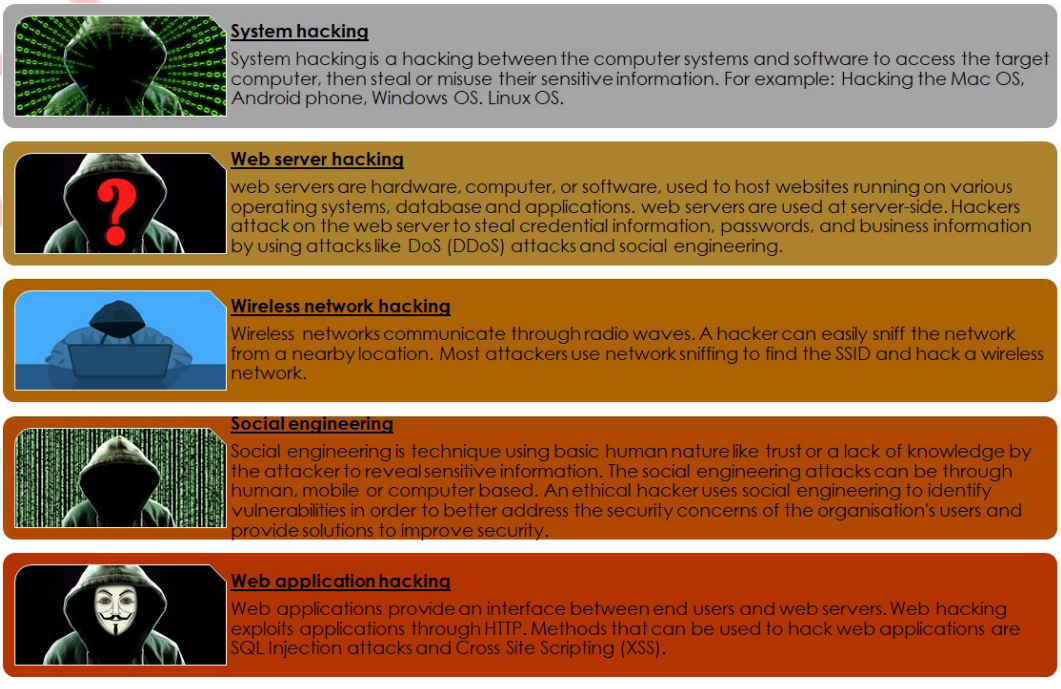


Figure 1.1.32 : Types of ethical hacking

Importance of ethical hacking

Cybercrime is steadily increasing. This is due to international conflicts and the role of cyber terrorists who attempt to hack national security systems in order to extort large sums of money by inserting malware and denying access. Every day, new worms, malware, viruses, and ransomware emerge. For example, many countries were affected by malware called 'darkhotel', which attempts to spy on corporate travellers and gain access through the hotel's WI-FI services. Before falling victim to a hacker, organisations must update their hack-prevention strategies and deploy different technologies to defend the system. Therefore, there is a need for ethical hacking services to safeguard the networks of businesses and the country.

An ethical hacker, when hacking a computer system, acts to be a security expert. They break into systems in order to detect threats and unauthorised access. They are continually come across with two obstacles - threat and weakness. Ethical hacking follows the guidelines of safe hacking. This is a complex procedure; therefore, an ethical hacker requires great skills to complete their job.

The fundamental benefit of ethical hacking is that it prevents malicious attackers from stealing and misusing data. A few points are listed below to understand more about the need for ethical hacking.

Ethical hacking helps to do the following.

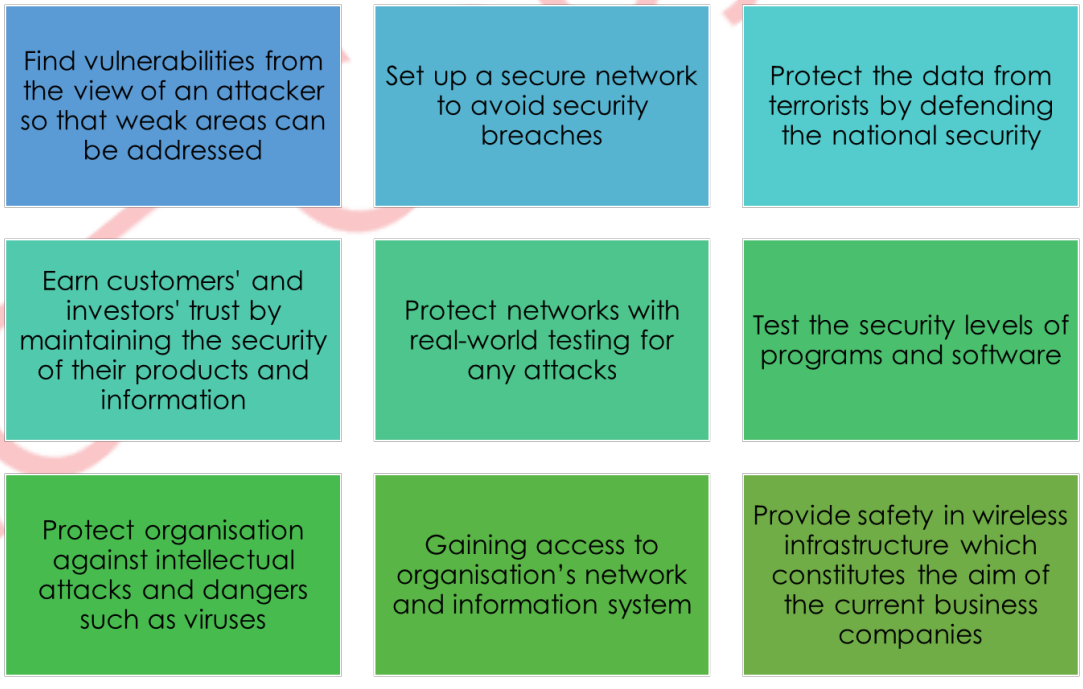


Figure 1.1.33 : Need for ethical hacking

The efficiency of an organisation's security should be evaluated on a regular basis. Ethical hacking solutions are the greatest technique to examine hacked systems and fine-tune any tiny flaws that could lead to any organisation security.

HB **Complete activity 1.1.10 in your workbook.**

Phases of ethical hacking

As you are aware now, ethical hacking is the process of identifying vulnerabilities in an application, system, or organisation's infrastructure that can be exploited by an attacker. Ethical hacking is also called penetration testing. In this process, an ethical hacker finds ways to prevent cyber attacks and security breaches by lawfully hacking into the systems and looking for weak points.

An ethical hacker follows the five-step hacking and thought process of a malicious attacker to gain authorised access and test the organisation's strategies and network. The ethical hacking process starts with looking for various ways to hack into the system, exploiting vulnerabilities, maintaining steady access to the system, and finally, clearing the user's tracks. The five phases of ethical hacking are:

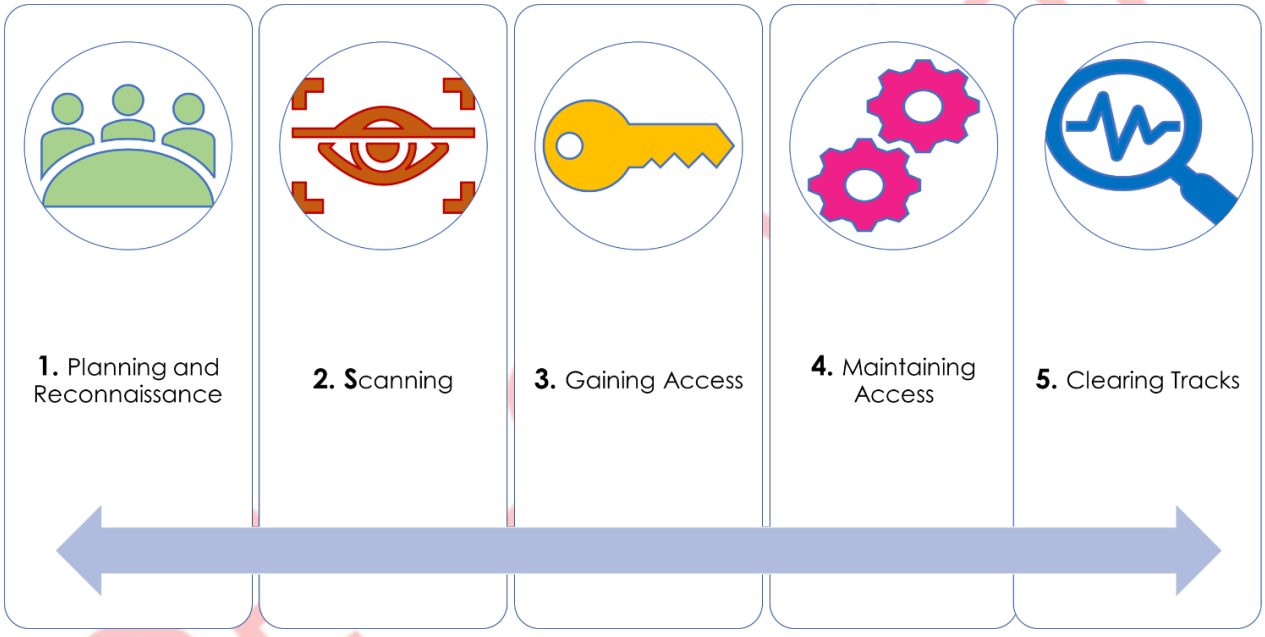


Figure 1.1.34 : Ethical hacking phases

Phase 1: Reconnaissance

The first phase and an essential phase in the ethical hacking process is **reconnaissance**. This phase is also known as the **footprinting** or information gathering phase, where the hacker gathers as much data as possible.

The attacker gathers all required information about the target before executing an attack. Passwords, employment information like name, email, date of birth, position, and other sensitive information are likely to be included in the data. The attacker can obtain information about an individual by utilising tools like:

- **HTTPTrack** to download a whole website and gather information about them
- Using search engines like **Maltego** to investigate them through numerous links, employment profiles, news, and so on.

Reconnaissance helps to identify which attacks are launched and how likely the organisation's systems fall vulnerable to those attacks. Footprinting collects data from areas such as:

- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) services
- Vulnerabilities
- Through specific IP addresses
- Host of a network

In ethical hacking, footprinting is of the following two types

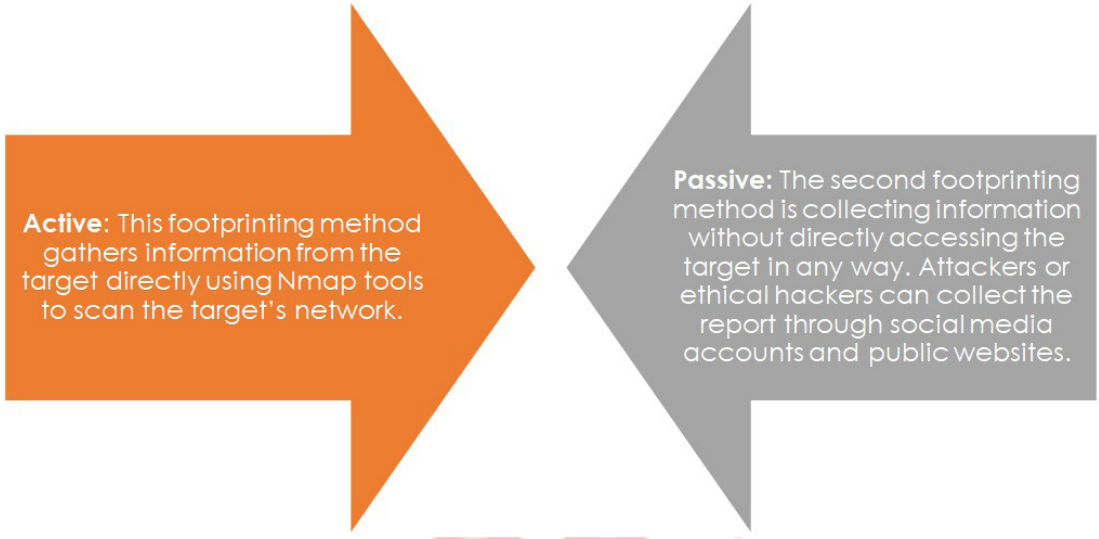


Figure 1.1.35 : Footprinting

Phase 2: Scanning

Scanning is the second step in the hacking process. In this phase, the attackers try a variety of methods to obtain the target's information. User accounts, credentials, and IP addresses are among the information targeted by the attacker. In this phase, hackers use tools such as port scanners, network mappers, and vulnerability scanners to find an easy and quick way into the network and skim for information. A few scanning techniques for ethical hacking that are employed in this phase are described below.

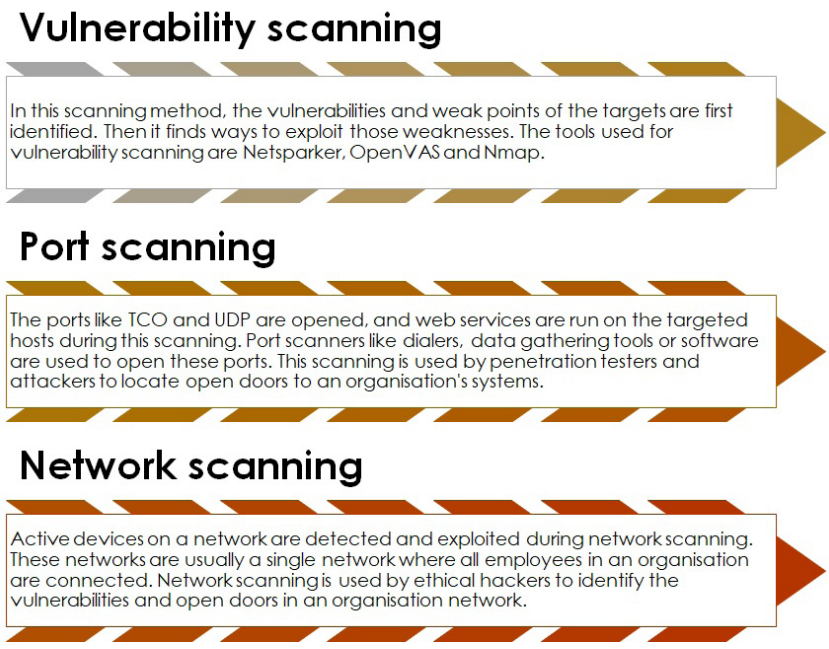


Figure 1.1.36 : Scanning

Phase 3: Gaining access

In the next stage of hacking, an attacker employs all means to gain unauthorised access to the target's systems, applications, or networks. To get access and penetrate a system, an attacker can utilise a variety of tools and approaches. This hacking phase tries to gain access to the system and exploit it by installing malicious software or applications, stealing sensitive data, gaining unauthorised access, demanding ransom, and so on.

Note: One of the most extensively used tools for gaining access is Metasploit. Also, social engineering is a regularly utilised technique to exploit a victim.

Ethical hackers and penetration testers use **passwords** to secure all systems and applications and protect potential entry points. To secure the network infrastructure, ethical hackers use a **firewall**. Ethical hackers also use social engineering techniques by sending fake social engineering emails to employees in order to identify which employees are most vulnerable to cyber attacks.

Phase 4: Maintaining access

Once the attacker has gained access to the target's system, the attacker makes every effort to keep the system. At this stage, the hacker continues to exploit the system. They execute DDoS assaults, use the hacked system as a launching pad, or steal the complete database.

Note: Backdoors and Trojans are tools that are used to exploit a weak or vulnerable system to steal credentials, important records, and other information.

The main goal of the attacker in this phase is to keep their unauthorised access until they finish their malicious operations without the victim noticing.

Ethical hackers or penetration testers can use this phase to scan the entire organisation's infrastructure for malicious activities and their root causes in order to prevent the systems from being exploited.

Phase 5: Clearing tracks

Hackers must remove their tracks in the final phase of ethical hacking, as no attacker wants to be detected. This procedure ensures that the attackers leave no traces or evidence that can be traced back to them. It is critical because ethical hackers must remain connected to the system without being detected by incident response or the forensics team.

Note: Editing, distorting, or deleting logs or registry values are examples. Additionally, the attacker deletes or uninstalls folders, apps, and software and guarantees that the modified files are traced back to their original value.

Ethical hackers use the following ways to erase their tracks:
- Using reverse HTTP Shells
- Deleting cache and history to erase the digital footprint
- Using ICMP (Internet Control Message Protocol) Tunnels

HB Complete activity 1.1.11 in your workbook.

Why footprinting is needed?

The main objective of footprinting is to get a complete view and as much information as possible about the specific target to set up the path that will be taken to execute the attack in a later phase. The information that the ethical hacker is trying to collect is network information, host (system information) and organisation information, as described in the following figure. The ethical hacker spends 90% of the time profiling an organisation and 10% launching the attack.

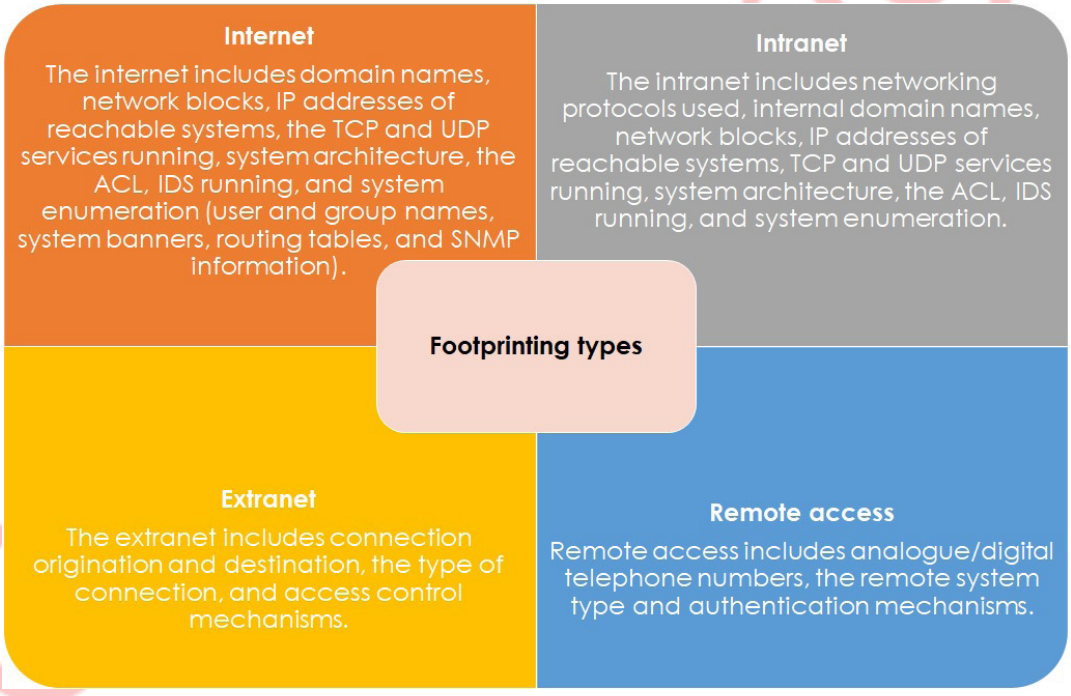


Figure 1.1.37 : Footprinting

Footprinting techniques/tools

There are different tools/techniques for identifying IP addresses, sub-domains, devices and technologies. Identifying sub-domains is usually the first step in passive footprinting. It is very important to determine sub-domains and net ranges associated with your target because it helps you to discover the scope of your other activities. WHOIS lookup and Netcraft are useful tools for gathering such information. Netcraft also provides information regarding various technologies that are used on websites, while the search engine tool will search for devices that are publicly exposed.

WHOIS Lookup technique

WHOIS lookup is a technique for gathering information in the footprinting phase. WHOIS information is based on a tree hierarchy. There are many WHOIS lookup tools available on the internet in the form of websites, but some operating systems like Windows and Linux have them in the form of a command-line program. WHOIS can reveal information about servers, which website is hosted and its location, and also display the name, address and contact numbers of technical staff, the domain owner and the domain registrar.

Whois lookup tool

For lookup in CLICK HERE , you can type in the domain name or IP address. When you perform a domain lookup, you get information regarding that domain. It will show you the domain, organisation, domain name server details, phone numbers, fax and other details. Sometimes it will show the administrator details, which can be very useful if you want to perform social engineering activities.

To search for a domain name registration record, enter the URL in the search field and

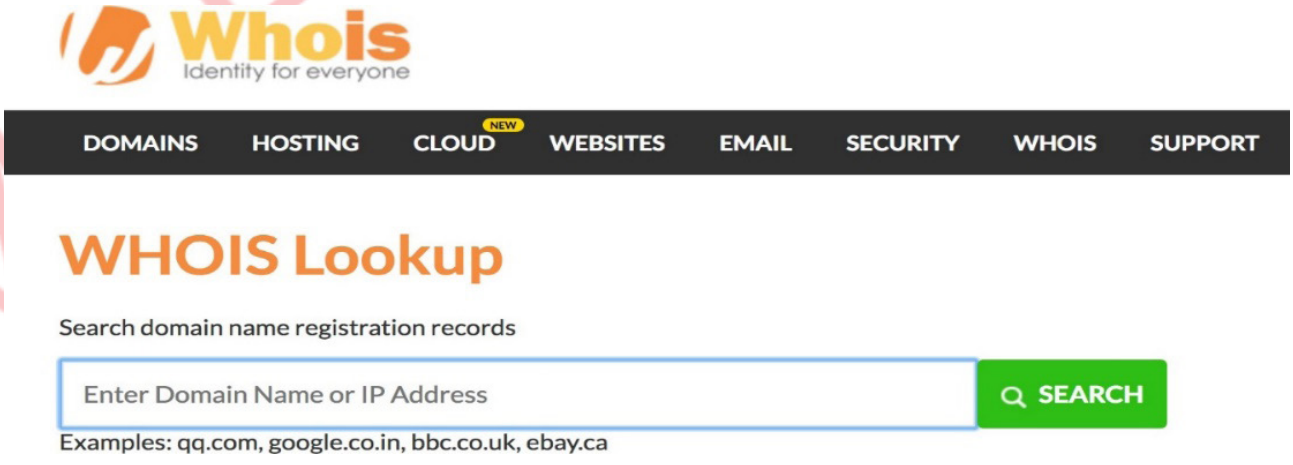


Figure 1.1.38 : WHOIS lookup

click on search.

WHOIS Command

For lookup in an operating system like Windows or Linux, you can type in the following command:

Syntax:

whois [URL]

Search Engine technique

Use a search engine to gather information about the target, such as technology platforms, employee details, login pages, intranet portals, and more. This can reveal a great amount of information and help the ethical hacker locate detailed information such as employee details, company policies and online hidden web pages. Any search engine has its own syntax. To search for and collect information, you can use some of the search operators/ commands listed below.

Search Engine Operators/Commands

Table 1.1.4

Operator /Command	Function	Example
Site:[URL]	List the available domains under the target site	site:futuresmarteducation.com
Site:[URL] ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini	List the publicity exposed configuration files	site:futuresmarteducation.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ora | ext:ini
Site:[URL] ext:sql | ext:dbf | ext:mdb	List the publicity exposed Database files	site:futuresmarteducation.com ext:sql | ext:dbf | ext:mdb
Site:[URL] ext:log	List the publicity exposed log files	site: futuresmarteducation.com ext:log
Site:[URL] ext:bkf | ext:bkp | ext:bak | ext:old | ext:backup	List the publicity exposed backup and old files	site:futuresmarteducation.com ext:bkf | ext:bkp | ext:bak | ext:old | ext:backup
Site:[URL] inurl:login	List of publicity exposed login pages	site: futuresmarteducation.com inurl:login
Site:[URL] ext:doc | ext:docx | ext:odt | ext:pdf | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv"	List of publicity exposed document files	site: futuresmarteducation.com ext:doc | ext:docx | ext:odt | ext:pdf | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv

Netcraft technique

Netcraft tool

This technique provides data about nearly every website and can be extremely useful for penetration testers. On the right side of the website, there is a prompt that asks: What is the site running? This is the Netcraft site's report toolbar in which you can type the domain or site, and it will return information about it. If you type in the domain, it will present the websites that are related to that specified domain. You can click on those websites to open a site report about them.

DNS footprinting – MX entry technique

Domain Name System (DNS) can reveal information about MX (host/domain) mail exchanges which indicates what email application services are being used. This information can be used later to exploit mail services and email accounts.

An example of a DNS lookup website is CLICK HERE which is used to search for a domain name and IP address.

Network technique

Ping Command

This command is used to extract the IP address and identify if the target site is online. Login onto the operating system commands prompt screen, and write Ping then the URL.

Syntax:
Ping [URL]

NSLOOKUP Command

This command helps us find DNS details, including IP addresses of a particular computer, mail exchange records for a domain and the DNS servers of a domain. The name nslookup means 'name server lookup'. Login onto the operation system commands prompt screen, and write server and the IP address.

Syntax:
Server [IP address]

Set q=mx Command

This technique is used to retrieve mail server information. You can use the following commands to get the mail server name.

Syntax:
Set q=mx

Social engineering technique

As you are aware, social engineering is the art of manipulating people to reveal confidential information and involves gaining their trust. Social engineering is a non-technical attack, but it involves tactics for trapping a victim. This is a technique used to gain important information about an organisation, such as the departments the employees belong to, their extension numbers, email addresses, and their job titles.

Why is scanning needed?

The main objective of scanning is to get more detail about the big picture and refine the path the ethical hacker started in footprinting which will be used to execute the attack later. Scanning allows the ethical hacker to do the following:

- Detect the live systems running on the network
- Discover which ports are active/running
- Determine the operating system running on the target system (fingerprinting)
- Identify the services running on the target system
- Discover the IP address of the target system

Scanning is necessary for network security assessment. Scanning is used to:
- Evaluate and audit the security of the firewall
- Identify unexpected new servers
- Identify open ports to protect the network from attacks

Types of scanning

There are three types of scanning:
1. Port scanning: is a series of messages sent to a computer to learn about services and scan its open ports. Through this scan, the ethical hacker can determine which port is vulnerable to attack.
2. Network scanning: a procedure for identifying active hosts on a network and for scanning IP addresses.
3. Vulnerability scanning: an automated process of proactively identifying vulnerabilities of computing systems.

Port scanning

Port scanning is one of the most popular techniques attackers use to discover services that they can exploit to break into systems. It is used by the ethical hacker to find the open doors and to find out the vulnerabilities in the services listed on a port.

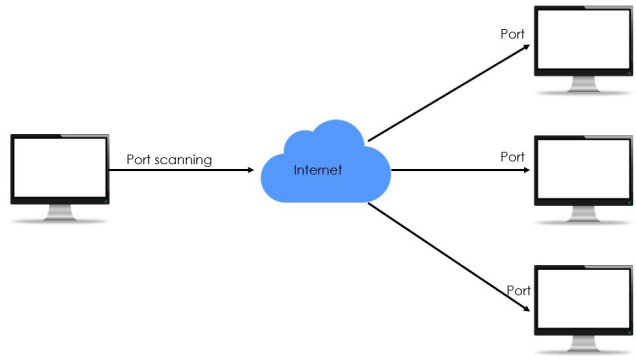


Figure 1.1.39 : Port scanning

Types of port scans include:

- **vanilla** - an attempt to connect to all 65,536 ports
- **strobe** - an attempt to connect to only selected ports (typically, under 20)
- **stealth scan** - several techniques for scanning that attempt to prevent the request
- for connection being logged
- **FTP bounce scan** - attempts that are directed through a file transfer protocol and
- server to disguise the hacker's location
- **fragmented packets** - scans by sending packet fragments that can get through simple packet filters in a firewall
- **UDP** - scans for open user datagram protocol ports
- **sweep** - scans the same port on many computers

Network scanning

In the footprinting phase, the ethical hacker creates a profile of the targeted organisation. This profile includes data such as the organisation's domain name system (DNS) and email servers, in addition to its IP address range. During the scanning phase, the ethical hacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their operating systems (OSs), the services running on every computer and active hosts on a network.

Figure 1.1.40 : Network scanning

The network port scan sends data packets via the network to a computing system's specified service port number (for example, port 23 for Telnet, port 80 for HTTP, and so on). This is to identify the available network services on that system. This procedure is effective for troubleshooting system issues or for tightening the system's security.

The purpose of network scanning is to:
- recognise available udp and tcp network services running on the targeted hosts.
- recognise filtering systems between the user and the targeted hosts.
- determine the operating systems (OSs) in use by assessing ip responses.
- evaluate the target host's tcp sequence number predictability to determine sequence prediction attack and TCP spoofing.

Vulnerability scanning

This is an automated process of proactively identifying vulnerabilities of computing systems in a network to determine if and where a system can be exploited or threatened. It is scanning of systems that are connected to the internet. Vulnerability scanning predicts the effectiveness of countermeasures by detecting specific weak spots in application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes.

Figure 1.1.41 : Vulnerability scanning

Types of vulnerability scanners include:

- Port scanner: probes a server or host for open ports.
- Network enumerator: a computer program used to retrieve information about users and groups on networked computers.
- Network vulnerability scanner: a system that proactively scans for network vulnerabilities.
- Web application security scanner: a program that communicates with a web application to find potential vulnerabilities within the application or its architecture.
- Computer worm: a type of self-replicated computer malware which can be used to find out vulnerabilities.

Scanning techniques/tools

Telnet commands

1. To check if a TCP port is open or reachable is to use the telnet command.

Syntax:

telnet [Host URL] [Port number] or telnet [IP address] [Specific port]

2. To search for open ports in one step, use the telnet command loop.

Syntax:

For /L % i in ([start port], [step], [end port]) do telnet [IP address] %i

3. To search for open range of port\s using the company URL for a specific accepted protocols (TCP,UDP) running behind the port, type:

Syntax:

portqry –n [URL] –p [protocol] –[port representation] port number

portqry: is a port query command.

- -n : specifies remote domain
- -p : TCP or\and UDP ; specifies accepted protocol running behind the port.
- -[port representation]: -e (single port), -r (port range), -o (specific multiple ports)

Banner grabbing

This is used to open a telnet connection to various TCP ports on the target system and to record the banner information that is presented

1. To identify web server OS, web server version and supported platform, type:

Syntax:

telnet [domain] [http port] OPTIONS / HTTP/1.0

2. To identify the SHH certificate, type:

Syntax:

telnet [domain] [SHH port]

3. To Identify the running operating system and FTP server version, type:

Syntax:

telnet [domain] [FTP port]

SYST

4. To identify the running mail server, type:

Syntax:

telnet [domain] [SMTP/POP3 port]

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1- .....

2- .....

3- .....

Two things I have enjoyed:

1- .....

2- .....

Learning outcome	Key skills (Please tick the box to show your understanding of the skills below).	I do not understand.	I understand.	I am an expert.
Show the different types of cyber attacks.	I can explain what is meant by cyber attack.			
	I can describe the common cyber attack types including DoS attack, password attack, and SQL injection attack.			
Illustrate the lifecycle of ethical hacking.	I can describe ethical hacking and its importance.			
	I can identify ethical hacking laws and guidelines.			
	I can identify and analyse the stages (Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Tracks) an ethical hacker requires to take in order to compromise a target system.			
Compare types of malicious software.	I can explain what is malicious software.			
	I can identify the common types of malicious software including viruses, worm, and trojan.			
Differentiate between passive and active attacks.	I can define passive attacks.			
	I can define active attacks.			

	I can differentiate between passive and active attacks on the basis of what are they, how they are performed and how much extent of damage they cause to the system resources.			
Categorise mobile security threats.	I can identify the common mobile security threats including unsecured Wi-Fi, network spoofing, and spyware.			
Teacher's comment:				

Section 2 : Cyber safety

Aim

In this section, you will learn about cyber safety and the rules to follow to prevent cyber attacks. You will be introduced to the different categories of cyber-security. You will get to know the three stands of security called the CIA triad, which will give an idea about confidentiality, integrity, and availability with respect to security.

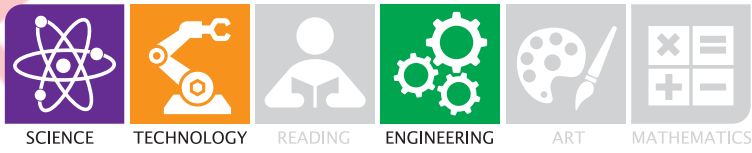
Learning outcomes

- Apply cyber-safety rules.
- Identify the different categories of cyber-security.
- Demonstrate confidentiality, integrity and availability (CIA) Triad.
- Discuss the techniques used to prevent cyber attacks.

Prior knowledge

- Computer Science
- Networking

My STREAM Focus



Key vocabulary

WORD	MEANING	PICTURE
cyber safety	safe and responsible use of information and communication technologies	

What is computer security?

Computer security is essential in the digital age. The technique of preventing and detecting illegal usage of your computer system is known as computer security. Computer security refers to the protection of computer systems and data against theft, harm and unauthorised access. There is a need to provide strong security to the computer system.

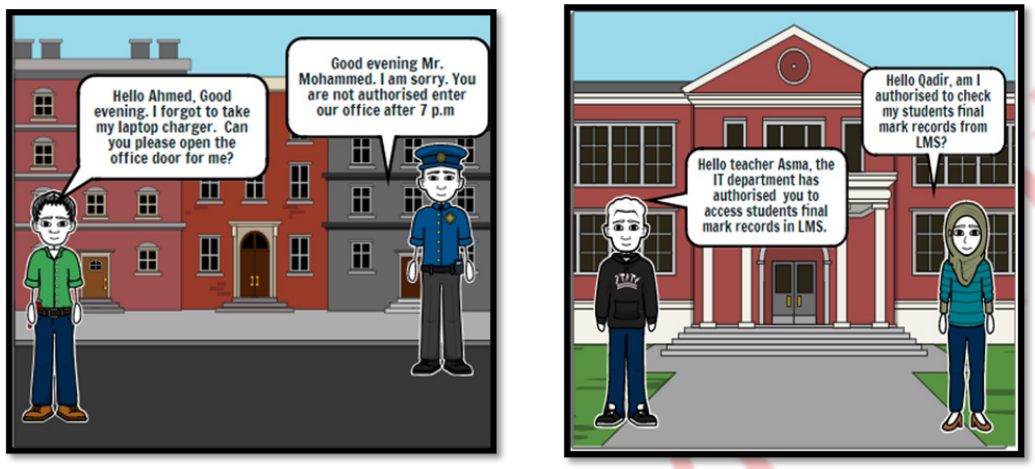


Figure 1.2.1 : Security

Cyber safety

Cyber safety means being secure online. Threats to safety and security exist in the online world. Everything that poses a risk, such as a publicly accessible internet connection, phishing emails, suspicious URLs, downloadable documents, or apps, is considered a threat. Because it is impossible to prevent all threats, cyber safety not only helps to avoid them but also to protect against their consequences. Even if someone follows all standard security precautions, they may still be the target of an attack.

CIA traid in security

As you clearly understand the different terms in security now, it is important to understand the CIA triad. Therefore, what is a CIA triad?

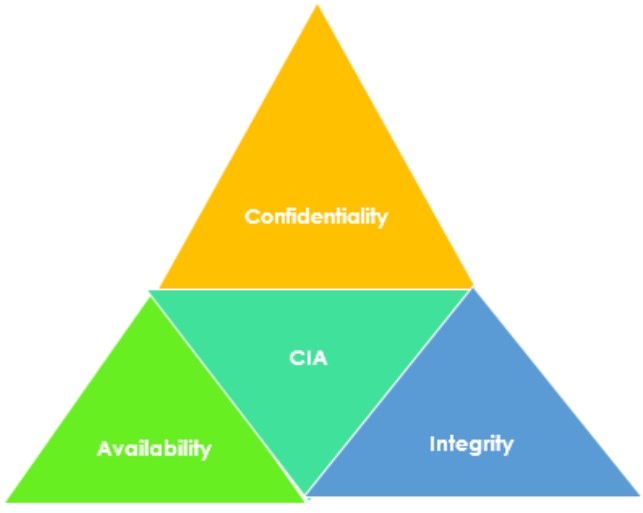


Figure 1.2.2 : CIA triad

CIA stands for **Confidentiality, Integrity** and **Availability**. These triads are explained as follows:

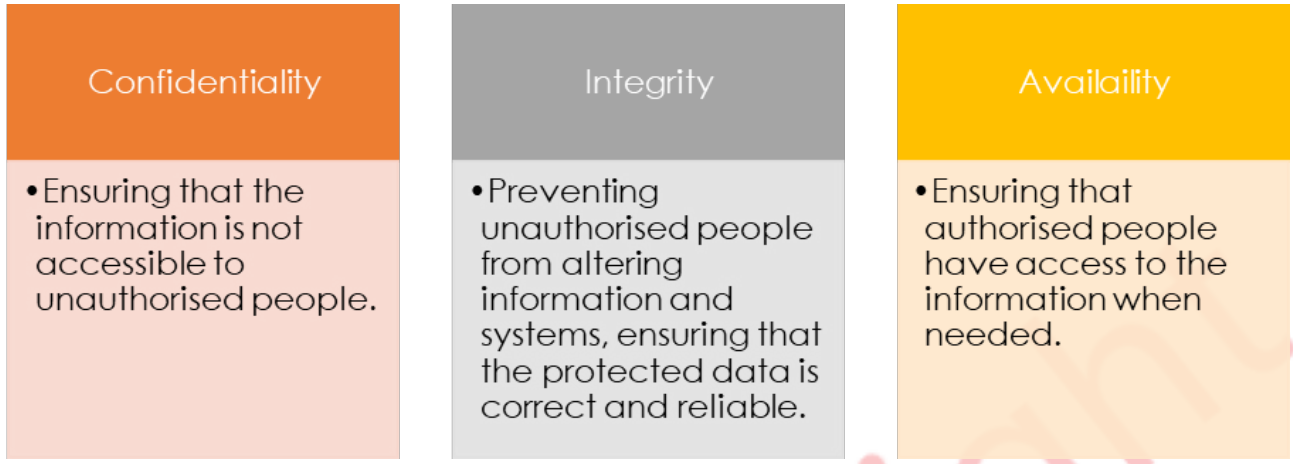


Figure 1.2.3 : CIA – Confidentiality, Integrity, Availablity

HB **Complete activities 1.2.1 and 1.2.2 in your workbook.**

Note:

What is an asset?
An asset is any data, device or other component of an organisation's systems that is valuable. Assets are valuable because they contain sensitive data that can be used to access sensitive information.

For example:
- An employee's desktop computer, laptop or company phone are assets.
- A company's network devices like servers, printers, computers, switches, and support systems, are assets.

Types of cybersecurity

Cybersecurity can be applied to a variety of categories in today's world of technology. They can be applied to user applications at the front-end, organisations policies and to the back-end network infrastructure. The most common categories of cybersecurity are:

1. Infrastructure security

Infrastructure security is the security level that relates to both hardware and software assets. This includes technology assets, such as computers, networking systems, and cloud resources.

Infrastructure security includes protection against traditional cyber attackss. This type of security also includes protection against natural disasters and other calamities like earthquakes or firebreaks down. Also, after a cyber attack, infrastructure security takes an important role in making an organisation recover and resume the normal workflow. From an enterprise or business point of view, infrastructure security focuses on improving security, reducing business downtime compliance costs, improving customer satisfaction, and reducing brand and reputation damage.

Levels of infrastructure security

In an organisation or an enterprise, the infrastructure security follows the below levels for securing.

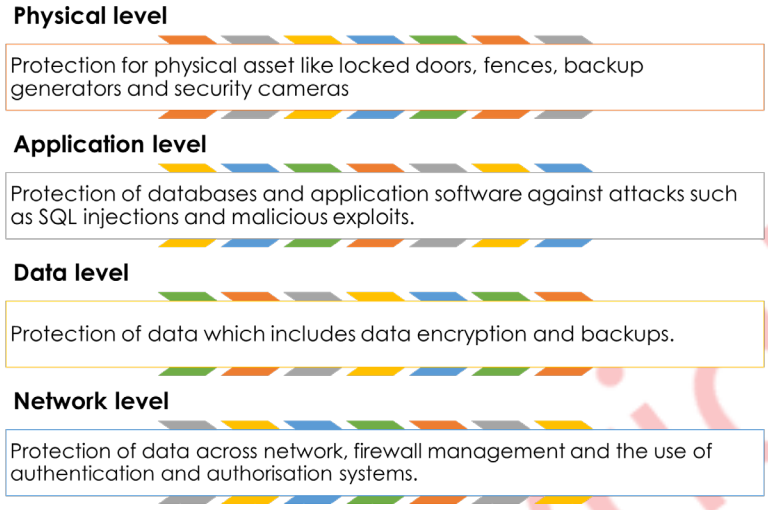


Figure 1.2.4 : Infrastructure levels

2. Network security

Network security is the process of taking physical and software preventative measures to protect the networking infrastructure from unauthorised access, misuse, malfunction, modification, destruction, or improper disclosure. Network security creates a secure platform for computers, users and programs to work within a secure environment.

The need for network security

Network security is important to protect users' data and information. Network security also secures shared data, ensures reliable access to the network, and protects the computer systems from cyber attacks.

There are many layers that need to be considered when securing a network. Security must be provided for all the layers. This is because an attack can happen in any layer. So, the network security hardware, software and policies must be designed to address each area.

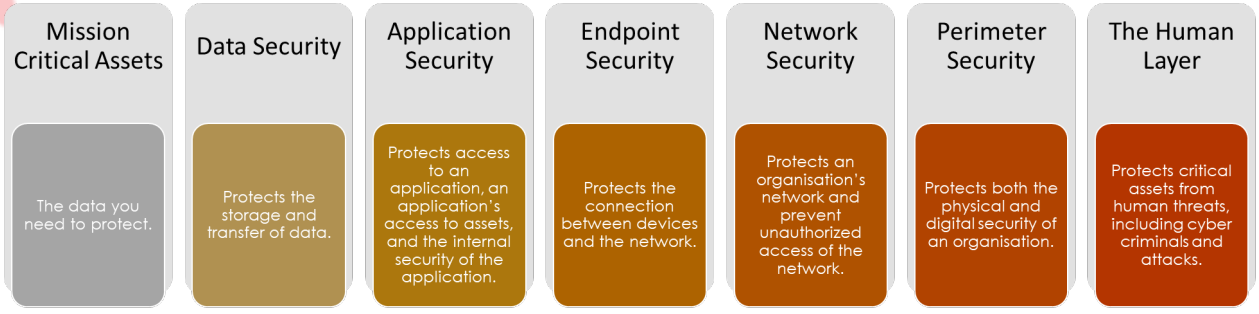


Figure 1.2.5 : Network security

Network security typically consists of three different controls as shown in the figure below.

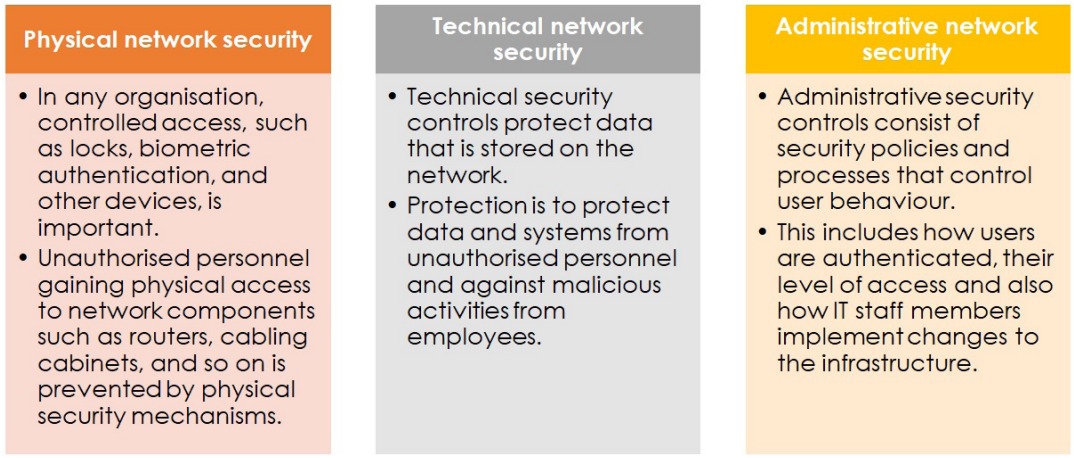


Figure 1.2.6 : Network security controls

A few common examples of network security implementation are listed below.
- Extra logins and new passwords
- Application security and internet monitoring tools
- Anti-virus and anti-spyware software
- Encryption and firewalls

3. Application security

Application security uses software and hardware methods to handle the external threats which can attack during the application development. As applications are accessible across networks, security measures must be implemented at the development phase of the project. Application security comes in a variety of forms like **anti-virus software, firewalls,** and **encryption** software. These software prevent unauthorised access. Organisations also attach specific application security processes to the **data sets** to protect organisations' sensitive data.

4. Cloud security

People always have thought that storing data in cloud computing is less secure than the traditional methods. People feel that storing data on physical servers and systems that they own and control is more secure. However, cloud security has proved that control does not imply that security and ease of access are more important than the actual location of your data.

Cloud security is a software-based security tool. This software monitors and protects the data stored in the cloud resources like servers. In today's technology market, cloud providers are constantly creating and implementing new security tools for cloud storages. This helps the enterprise users to secure the organisation's data.

Did You Know

According to a recent cloud security report, users in on-premises environments experience more breaches at an average of 64.4, and those in cloud service provider environments face an average of 27.8 attacks. Therefore, in cloud computing, the risk of security breaches is minimal.

5. Internet of things (IoT) security

As you are aware, the Internet of Things (IoT) connects billions of physical devices across the world to the internet to collect and share data. These devices include home appliances (television), sensors, wi-fi routers, cameras, and printers.

Did You Know

The Internet of Things is expected to increase to $520 billion by 2021 onwards, which is more than doubling the $235 billion spent in 2017.

IoT security is very important because IoT devices are frequently in a vulnerable state with little to no security patching. All IoT users encounter various security challenges because of this. According to research, it has been found that:

- organisations would acquire more IoT devices on average if IoT security issues were resolved.
- enterprises are positive about IoT's business value and growth if security issues were addressed.

Today IoT devices cannot be avoided. Therefore, it is essential to provide IoT security to all IoT devices.

Security threats

A security threat is an act that attempts to corrupt or steal data, disrupt an organisation's systems or the entire organisation. Security threats from network intruders can come from both internal and external sources, as shown in the following figure.

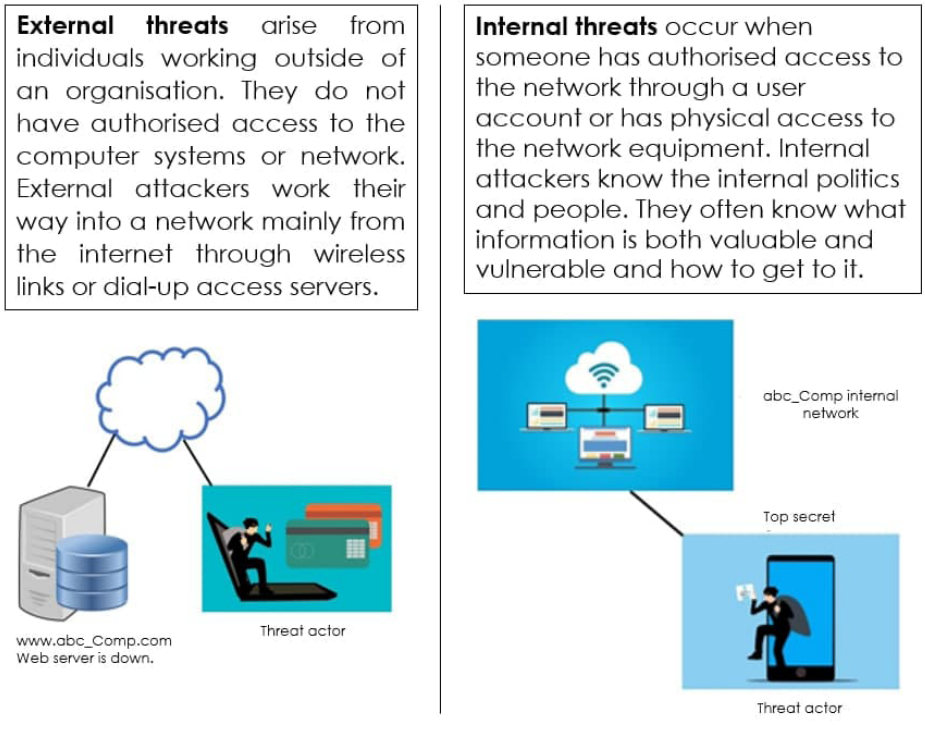


Figure 1.2.7 : Internal and external threats

Security threats categories are under the following four types.

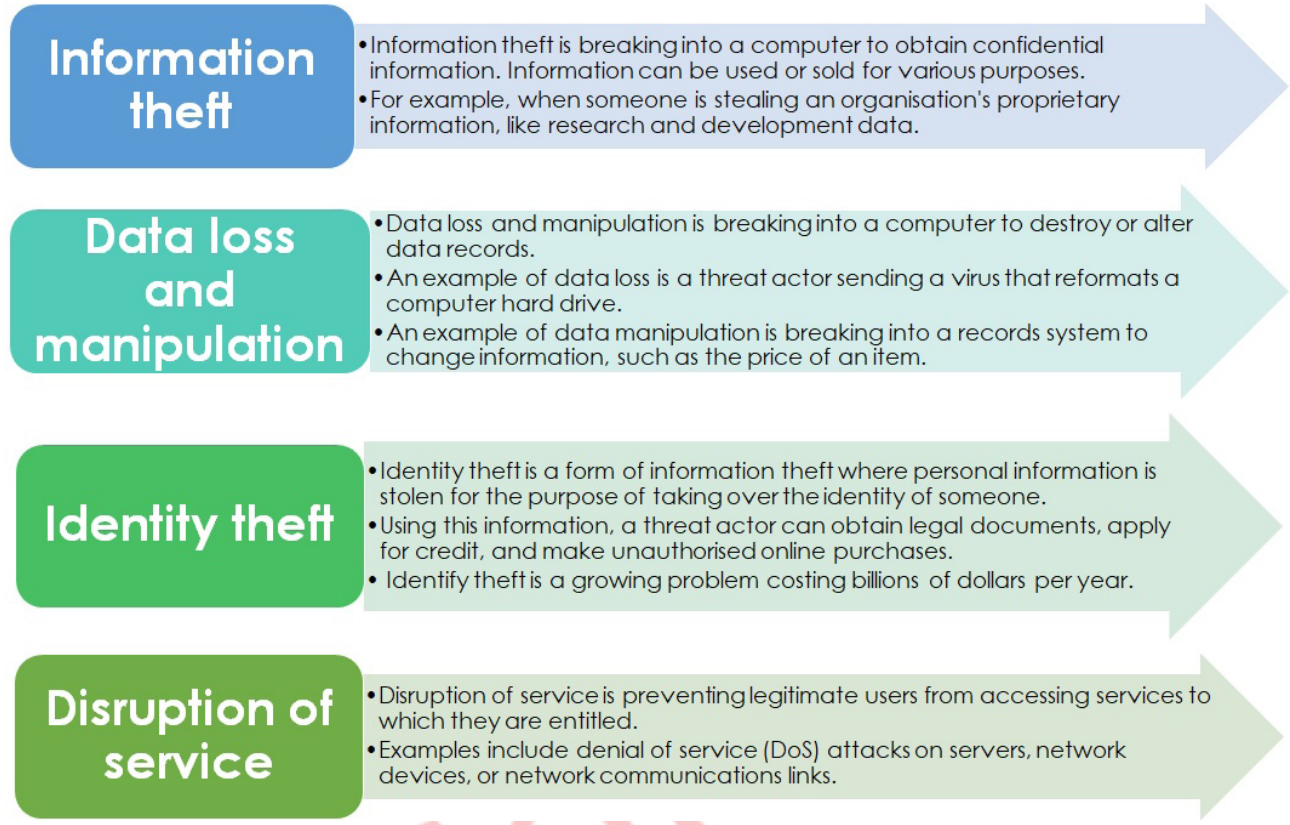


Figure 1.2.8 : Security threats

HB **Complete activity 1.2.3 in your workbook**

Cybersecurity vulnerability

Vulnerable means weakness. A security vulnerability is a weakness, flaw, or error found within a security system. A cybersecurity vulnerability is any weakness within an organisation's information systems, internal controls, or system processes that can be exploited by cybercriminals.

Common types of cybersecurity vulnerabilities

1. System misconfigurations

Configuration is the way parts are arranged to work together. Network assets with vulnerable settings or different security policies might cause system misconfigurations. If the system is misconfigured, the system becomes vulnerable. Hackers, who illegally gain access to systems, always look for system misconfigurations and vulnerabilities to attack.

Figure 1.2.9 : A hacker who tries to illegally gain the system access

The risk of network misconfiguration grows as more organisations use digital solutions. As a result, when installing new technology, businesses must engage with experienced **security specialists.**

Figure 1.2.10 : A network security specialist

2. Out of date or unpatched software

A **patch** is a set of changes to a computer program designed to update, fix, or improve it. For example, you are doing patching when you update an operating system on your mobile phone

or a computer. Like system misconfigurations, hackers probe networks looking for unpatched systems for attacking and stealing valuable information like passwords or company confidential data.

To limit this risk, a patch management schedule is required. This schedule will keep track of all new system patches to be implemented as soon as they are released.

Figure 1.2.11 : Software update

3. Missing or weak authorisation credentials

Common tactic attackers employ is to brute force their way into a network by guessing employee credentials. It is important to educate employees on cybersecurity best practices so that their login information cannot be easily exploited to gain access to a network.

4. Malicious insider threats

Whether unknowingly or with malicious intent, employees who have access to critical systems can share information that allows cybercriminals to breach a network. Insider threats can be difficult to track since all actions taken by employees will appear legitimate and therefore raise little to no red flags. To help combat these threats, consider investing in network access control solutions, and segment your network based on employee seniority and expertise.

5. Missing or poor data encryption

Networks with missing or poor encryption allow attackers to intercept communication between systems, leading to a breach. When poorly or unencrypted information is interrupted, cyber adversaries are able to extract critical information and inject false information onto a server. This can undermine an organisation's cybersecurity compliance efforts and lead to substantial fines from regulatory bodies.

6. Zero-day vulnerabilities

Zero-day threats are specific software vulnerabilities that are known to the attacker but have not yet been identified by an organisation. This means that there is no available fix since the vulnerability has not yet been reported to the system vendor. These are extremely dangerous as there is no way to defend against them until after the attack has been carried out. It is important to remain diligent and continuously monitor your systems for vulnerabilities in order to limit the likelihood of a zero-day attack.

Internet safety

The act of being secure online is known as **internet safety**. This includes being aware of the dangers that come with your online activities and implementing a few solutions to prevent or eliminate these dangers. Internet security is sometimes known as online safety, cyber safety, or e-safety.

Rules for internet safety

Figure 1.2.12 : Internet safety

Unsafe internet browsing can lead to many threats. Hackers will always be looking for personal information that they can use to gain access to your credit card and bank accounts. Unsafe browsing can also lead to other dangers, such as humiliating personal comments or photographs that are nearly impossible to remove once they have been posted online or getting mixed up with people you would have rather ignored. Here are a few basic internet safety rules to follow.

- Do not disclose any personal information
- Always keep your privacy setting ON
- Use secure websites for online shopping and payments
- Always keep your antivirus software updated
- Practice safe browsing
- Use secure VPN for secure internet connection
- Be careful when you download from internet
- Remember to use strong passwords
- Be careful on what you post
- Be careful on whom you meet online

Figure 1.2.13 : Rules for internet safety

Note:

UAE Cyber Privacy
Article 21:
It is also illegal to invade someone's privacy by:

- Eavesdropping, recording, transferring conversations communications, or materials
- Photographing others
- Publishing news, photos comments, or information even if true and correct.

It is essential to think carefully before acting online. Below are a few actions that may result in legal implications according to UAE's cybercrime law:

- Sharing and posting photographs and media: be careful before posting images that include other people without their consent. This is a criminal offence that breaches other people's privacy.
- Privacy and confidentiality: disclosing private or confidential information about an individual or organization without consent can result in legal implications.
- Offensive emoticons and emojis: Refrain from using culturally offensive emojis in social media conversations. This can result in serious complaints from the recipient even if it was intended as a joke.
- Defamation: or ruining an individual's reputation by sharing content that provokes public disapproval or contempt is a strict criminal offence.
- Immoral, offensive content that shakes social cohesion: any content that is "inconsistent with public morals and good conduct including content that is un-Islamic, blasphemous, lewd, that encourages sinful activity, or that is aimed at corrupting minors, etc." can have legal implications.
- Hacking and Malicious codes: "UAE TRA monitors online content available and prohibits content for hacking and malicious codes, Internet content providing unlicensed VoIP services and other illegal Internet content."

Note:

Strict penalties against cybercrimes in the UAE:

- "Those caught gaining access to a website, network or system without authorization are to be imprisoned and fined at least Dh50,000, but fines can go as high as Dh1 million if personal information is stolen or deleted."
- "Those caught using technology to invade someone else's privacy - which can even include eavesdropping, copying photos or publishing news - can be jailed for six months and face fines of between Dh150,000 and Dh300,000."
- "The most severe penalty - five years in jail and a Dh3 million fine - is reserved for those who run malicious software that causes a network or IT system to stop functioning 'or results in crashing, deletion, omission, destruction and alteration of the program, system, website, data or information'."
- "Additionally, the law stipulates various penalties for a number of other cybercrimes, including insulting religions and their rituals, slandering public officials, forging electronic official documents, sending or re-publishing pornographic materials, reproducing credit or debit card data, and obtaining secret pin codes or passwords"

Right to block online content: "Licensed service providers (Du and Etisalat) can also block online content if required and subsequent to complaints of abuse or defamation, authorities can take legal action against those running the sites after verifying the validity and seriousness of the complaint."

Security tools and applications

Internet security is a major concern around the world. As a result, many tools are available to network users to protect the devices from attacks and help remove malware from infected machines. Some of the security tools and applications used in securing a network are briefly described in the table.

Table 1.2.1

Security Tool or Application	Description
Firewall	A security tool that controls traffic to and from a network.
Patches and updates	Software that is applied to an OS or application to correct a known security vulnerability or add functionality.
Virus protection	Anti-virus software is installed on an end-user workstation or server to detect and remove viruses, worms, and Trojan horses from files and email.
Spyware protection	Anti-spyware software is installed on an end-user workstation to detect and remove spyware and adware.
Spam blocker	Software is installed on an end-user workstation or server to identify and remove unwanted emails.
Pop-up blocker	Software is installed on an end-user workstation to prevent pop-up and pop-under advertisement windows from displaying.

Example for patches and updates

A threat actor gains access to hosts or networks through software vulnerabilities. It is important to keep software applications up-to-date with the latest security patches and updates to help deter threats.

- A patch is a small piece of code that fixes a specific problem.
- An update includes additional functionality to the software package as well as patches for specific issues.

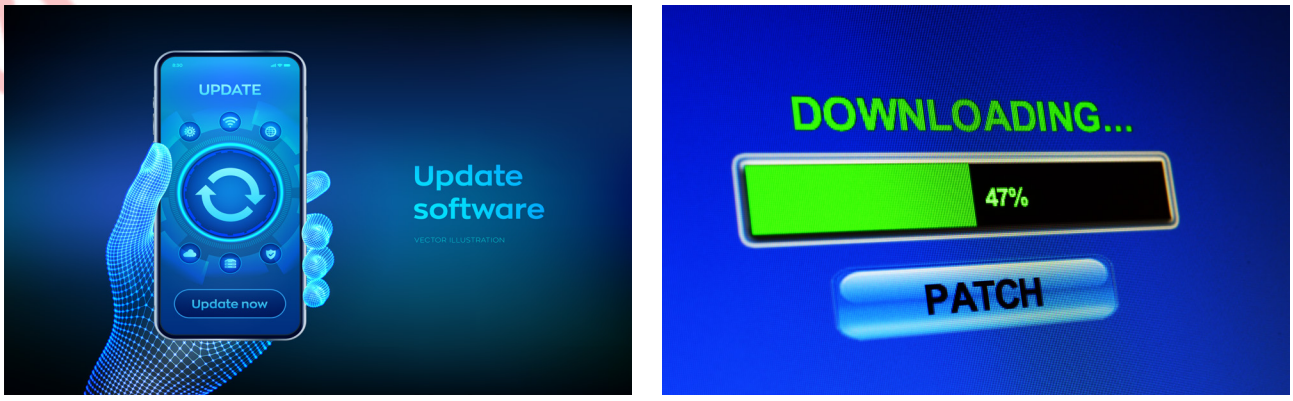


Figure 1.2.14 : Patch and update

OS and application vendors continuously provide updates and security patches that can correct known vulnerabilities in the software. Operating systems offer an automatic update feature that allows OS and application updates to be automatically downloaded and installed on a host.

Windows 10 Update Settings

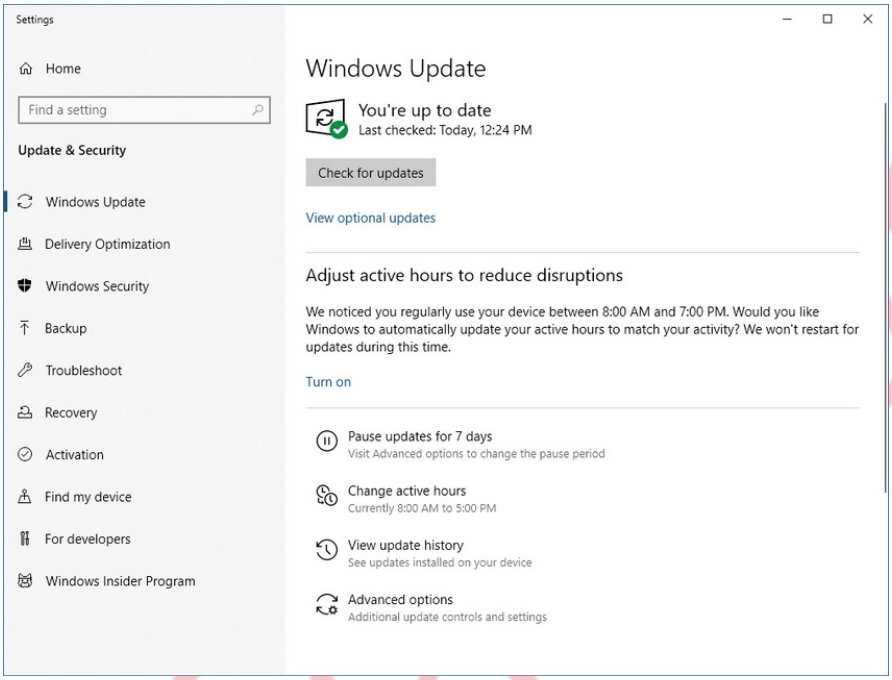


Figure 1.2.15 : Windows update settings

HB **Complete activities 1.2.4 and 1.2.5 in your workbook.**

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1- .....

2- .....

3- .....

Two things I have enjoyed:

1- .....

2- .....

Learning outcome	Key skills (Please tick the box to show your understanding of the skills below).	I do not understand.	I understand.	I am an expert.
Apply cyber-safety rules.	I can identify Internet safety rules to build awareness of possible internet dangers.			
Identify the different categories of cyber-security.	I can identify the 5 main types of cyber security including critical infrastructure security, application security, network security, cloud security, and IoT security.			
Demonstrate confidentiality, integrity and availability (CIA) Triad.	I can identify the information security goals in an organisation.			
Discuss the techniques used to prevent cyber attacks.	I can identify and report suspicious cyber events.			
	I can explore intrusion detection and prevention.			
Teacher's comment:				

Section 3 : Cyber security ethics

Aim

This section will introduce you to cyber security ethics. You will learn the legal and ethical issues that are involved in cyber attacks. You will also learn about data privacy and how data privacy is a concern when data is collected or generated in real-time.

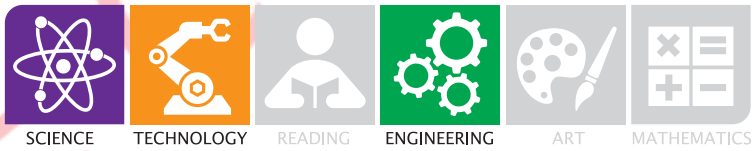
Learning outcomes

- Illustrate the legal and ethical issues that shape computing practices.
- Explain the privacy concerns related to the collection and generation of data.

Prior knowledge

- Computer Science
- Networking

My STREAM Focus



Key vocabulary

WORD	MEANING	PICTURE
cyber ethics	set of moral rules or a code of behaviour applied by online users to the online environment	

Ethics

Ethics is the study of what is right or wrong in human conduct. To understand ethics, you need to know the difference between ethics and morals.

Figure 1.3.1: Ethics

Ethics
- Ethics are the guiding principles that help the individual or group decide what is good or bad.
- Ethics are generally uniform.
- Ethics are abstract.
- Ethics has got the freedom to think.
- Some ethical principles are with lessons such as 'Do not take what does not belong to you' and 'Do not harm others'.

> Be truthfulness
> Be honest
> Be reliable
> Respect all
> Be Fair
> Integrity

An example of an unethical act:
Saif lost his science book. He finds Abdul's book in the school corridor. Saif decides to keep the book for himself without handing it to school's lost and found department.

Morals

- Morals are the beliefs of the individual or group as to what is right or wrong.
- Morals may differ from society to society and culture to culture.
- Morals are expressed in the form of general rules and statements.
- Morals have got no freedom to think.
- Some moral principles are:
    - > Do not cheat
    - > Be loyal
    - > Be patient
    - > Always tell the truth
    - > Be generous

Figure 1.3.2: Moral

An example of an immoral act:

Khadeja shares personal information with Reem, asking her to keep the secret confidential to herself. Reem ignored Khadeja's request and shared her personal information with Amal.

Cyber ethics

'Cyber ethics' refers to the code of responsible behaviour on the internet. Now that you have learned about ethics as a responsible act in everyday life, you should act responsibly in the cyber world as well.

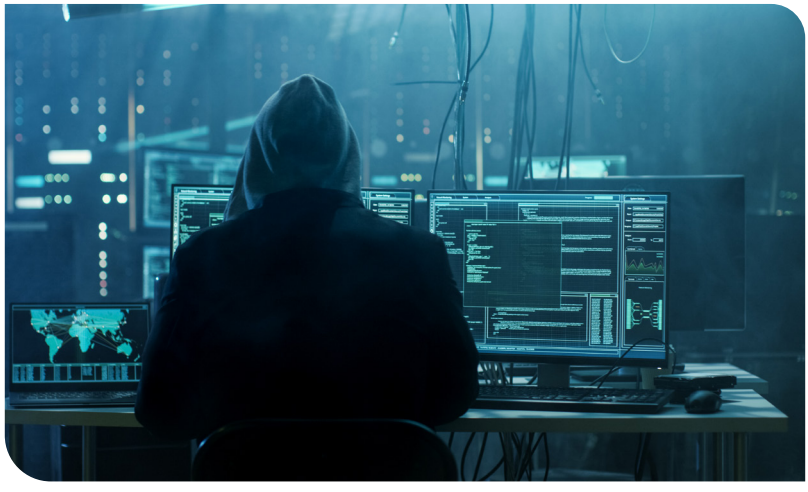


Figure 1.3.3: Cyber ethics

As a responsible cyber user, you should follow the following cyber ethics.

> Do not use someone else's password.
> Do not use rude or offensive language.
> Do not cyberbully.
> Do not copy information from the internet and claim it as your own. This is plagiarism.
> Do not break into someone else's computer.
> Do not attempt to infect someone else's computers.
> Do not damage someone else's computer to make it unusable.
> Strictly follow the copyright restrictions when downloading material from the internet that includes software, games, movies, or music.

Data privacy

Data privacy, often known as **information privacy**, is a component of information technology (IT) that deals with an organisation's or an individual's ability to decide which data in a computer system can be shared with third parties/public.

Figure 1.3.4: Data privacy

Why is data privacy important?

Wrong things can happen when data that should be kept private falls into the wrong hands.

- A data breach at a government agency, for example, may provide attackers access to top-secret material. A data breach at a company can put confidential information in the hands of a competitor.
- A school security breach might put kids' personal information in the hands of attackers who could use it to commit identity theft.
- Personal health information can fall into the wrong hands if a hospital or doctor's office suffers a data breach.

Protecting personal data

Government organisations and businesses invest millions of dollars each year to help protect their data. But average consumers like the common people cannot spend that amount of money on protecting their personal data. However, the following suggestions can help individuals protect their personal data.

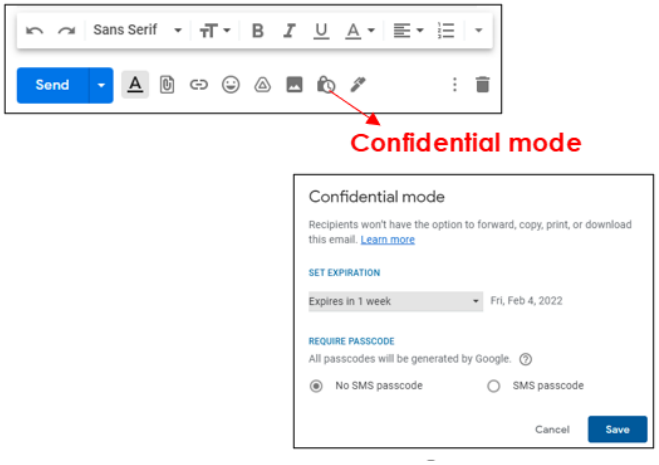
- Use strong, unique passwords for all of your online accounts.
- Use the security options provided by email services. For example, when using Gmail, you can send attachments with confidential mode 'on' to protect the information so that thieves cannot steal your mail.
- Shred documents that include receipts, bank and credit card statements, that contain personal information before discarding.
- Secure your home Wi-Fi network and other devices so that criminals cannot 'eavesdrop' on your online activity.
- Do not share your personal information if someone asks. Investigate why and for what purpose that person needs your personal information.

Figure 1.3.5: Paper shredding

Note:

Steps to send attachments with confidential mode using the email service Gmail.

1. On your computer, go to Gmail.
2. Click Compose.
3. Click Attach.
4. Choose the files you want to upload.
5. In the bottom right of the window, click Turn on confidential mode Turn on confidential mode.
6. Set an expiration date and passcode.
7. If you choose 'No SMS passcode,' recipients using the Gmail app will be able to open it directly. Recipients who don't use Gmail will get emailed a passcode.
8. If you choose 'SMS passcode,' recipients will get a passcode by text message. Make sure you enter the recipient's phone number, not your own.
9. Click Save.



Social media privacy issues

In recent years, social media users' concerns about their privacy have increased. Data breaches have shocked many users. In fact, this is forcing social media users to reconsider their social network interactions and the security of their personal information.

Figure 1.3.6: Social media

For example, the story of Cambridge Analytica explains privacy issues clearly. This business used the personal information of over 50 million Facebook users to sway the 2016 presidential election in the United States. Few other incidents like this had lost public's trust, leaving many people questioning if they have lost control over their personal data. According to a recent survey, 80 per cent of social media users are concerned about corporations and advertising accessing and utilising their posts on social media. As a result of these expanding privacy issues, organisations are demanding stricter laws.

Threats to privacy on social media

Figure 1.3.7: Privacy setting

Cyber criminals are skilled at tricking social media users into disclosing critical information, stealing personal data, and getting access to accounts that are thought to be private. The following are some of the most common social media threats.

Data mining

On the internet, everyone leaves a data trail or footprint. For example, when a new user opens a new social media account, they are required to enter personal information such as their name, birth date, geographic location, and personal interests. Companies also collect information on user activities, such as when, where, and how users interact with their platforms. Companies store and use all this information to target advertisements. Users' data is sometimes shared with third-party organisations without their knowledge or consent.

Phishing attempts

Phishing is one of the most frequent methods used by cybercriminals to obtain sensitive personal information. A phishing attack masks itself as a communication from a reputable company and sends it via email, text message, or phone call. These communications encourage recipients to share sensitive information such as passwords, banking information, or credit card numbers. Phishing attacks frequently take the shape of social media platforms. A huge phishing attempt attacked Instagram users in August 2019, acting as a two-factor authentication system and directing visitors to a fake Instagram page.

Malware sharing

Malware (malicious software) can be used to steal personal information (spyware), extort money (ransomware), or profit from forced advertising once it has infected a user's machine (adware). Malware distributors find social media sites to be a perfect delivery system. Once an account has been compromised (typically by phishing for passwords), cybercriminals can take control of it and use it to spread malware to all of the user's friends or contacts.

Botnet attacks

Whenever a new term is used in social media, the social media bots try to create posts or automatically follow new people. A botnet is a network made up of a huge number of bots. Bots and botnets are widely used on social media to steal data, spread spam, and execute distributed denial-of-service (DDoS) assaults that aid cybercriminals in gaining access to people's devices and networks.

HB **Complete activity 1.3.1 in your workbook.**

Laws governing data privacy

As technology advancements have enhanced data collection and surveillance capabilities, governments around the world have begun to pass rules governing what data can be gathered on users, how that data can be used, and how that data should be stored and safeguarded.

Figure 1.3.8: Privacy setting

The following are some essential regulatory privacy frameworks to be aware of:

1. U.A.E data office

The Personal Data Protection Law constitutes an integrated framework to ensure the confidentiality of the information and protect the privacy of individuals in the U.A.E. The UAE Data Office acts as the federal data regulator in the UAE. The office which is affiliated with the UAE Cabinet is responsible for:

- preparing policies and legislations related to data protection.
- proposing and approving the standards for monitoring Personal Data Protection Law.
- preparing systems for complaints and grievances related to data.
- issuing guidelines and instructions for the implementation of the law.

Protecting data and privacy online

U.A.E Federal Law No. 5 of 2012 on combatting cybercrimes makes it illegal to disclose any information obtained by electronic means if such information was obtained in an unauthorised manner.

- **Article 21** of the law makes one liable if he uses an electronic information system or any information technology means for offending another person or for attacking or invading his privacy.

- **Article 22** of the same law makes one liable if uses without authorisation, any computer network, website or information technology means to disclose confidential information which he has obtained in the course of or because of his work.

2. **General Data Protection Regulation (GDPR)** regulates how the personal data of European Union (EU) data subjects, meaning individuals, can be collected, stored, and processed, and gives data subjects rights to control their personal data.

3. **National data protection** laws regulate countries, such as Canada, Japan, Australia, Singapore, and others, to have comprehensive data protection laws in some form. Some, like Brazil's General Law for the Protection of Personal Data and the UK's Data Protection Act, are quite similar to the GDPR.

4. **California Consumer Privacy Act (CCPA)** regulates how consumers can be made aware of what personal data is collected and gives consumers control over their personal data, including a right to tell organisations not to sell their personal data.

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1- .....

2- .....

3- .....

Two things I have enjoyed:

1- .....

2- .....

Learning outcome	Key skills (Please tick the box to show your understanding of the skills below).	I do not understand.	I understand.	I am an expert.
Illustrate the legal and ethical issues that shape computing practices.	I can discuss the important ethical issues in cyber-security.			
	I can identify ethical best practices in cyber-security.			
Explain the privacy concerns related to the collection and generation of data.	I can discuss privacy concerns caused by data collection such as social media sites mining and surveillance videos.			
Teacher's comment:				

MOEUAEofficial