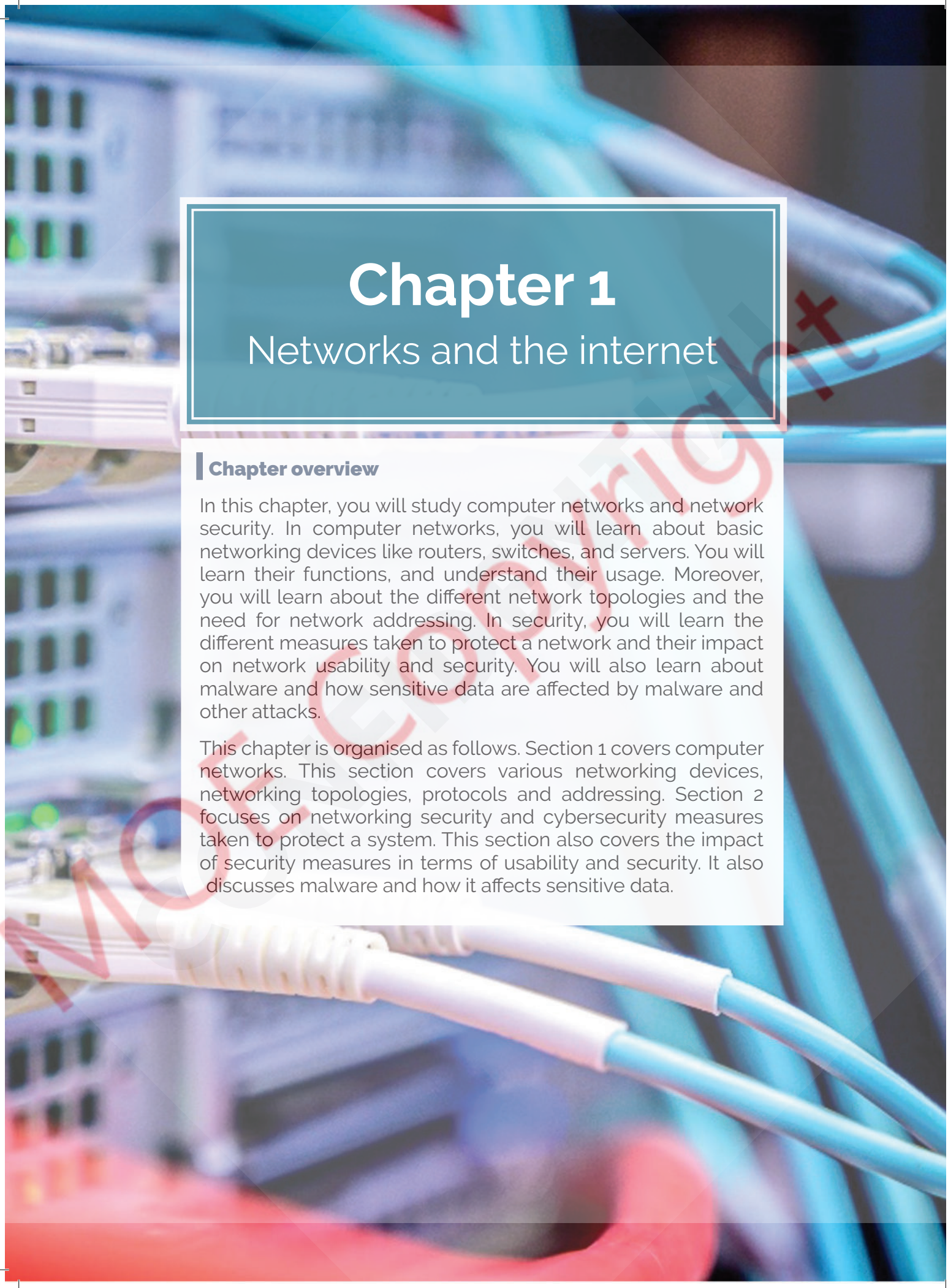
UNITED ARAB EMIRATES
MINISTRY OF EDUCATION

Networks and The Internet

Cycle 3 – Grade 9



Chapter 1

Networks and the internet

Chapter overview

In this chapter, you will study computer networks and network security. In computer networks, you will learn about basic networking devices like routers, switches, and servers. You will learn their functions, and understand their usage. Moreover, you will learn about the different network topologies and the need for network addressing. In security, you will learn the different measures taken to protect a network and their impact on network usability and security. You will also learn about malware and how sensitive data are affected by malware and other attacks.

This chapter is organised as follows. Section 1 covers computer networks. This section covers various networking devices, networking topologies, protocols and addressing. Section 2 focuses on networking security and cybersecurity measures taken to protect a system. This section also covers the impact of security measures in terms of usability and security. It also discusses malware and how it affects sensitive data.

Section 1: Computer networks

Aim

In section 1, you will learn about networking devices like routers, switches, and servers. You will learn the use of networking devices and their various functions. You will also gain an understanding of network topology, protocols, and network addressing.

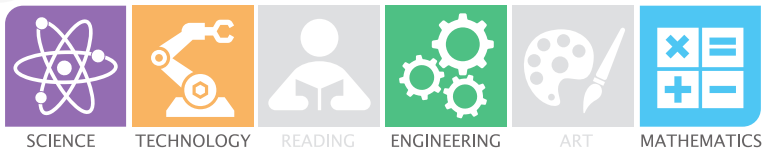
Learning outcomes

- Explain the relationship between routers, switches, servers, topology, protocols and addressing.
- Implement networks using a range of hardware, topologies, protocols and addressing.

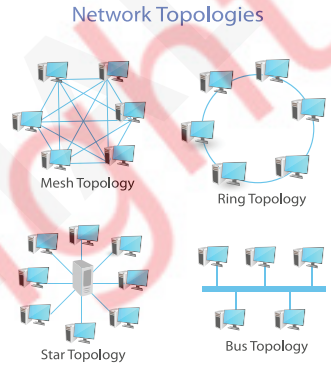
Prior knowledge

- Computer science
- Basics networking and network connections
- Devices used in networking
- IP addressing and protocols

My STREAM focus



Key vocabulary

WORD	MEANING	PICTURE
network	two or more computers that are linked in order to share resources	
topology	refers to how various devices, and connections on your network are physically or logically arranged in relation to each other	
protocol	set of rules that determine how data is transmitted between different devices in the network	
network address	unique identifier for a device on a network	

What is a network?

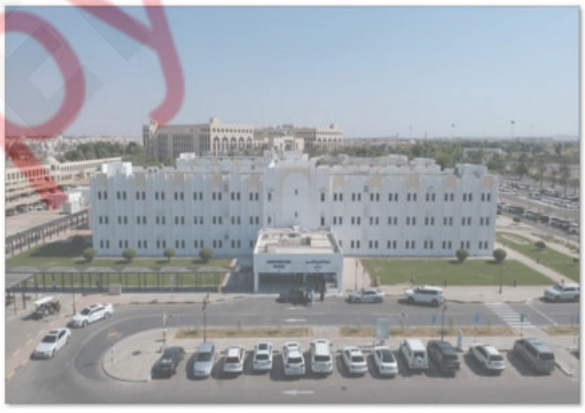
The network is important to interact with devices or people to exchange information and develop professional and social contacts. The term **'network'** refers to a group of two or more similar things or individuals that are interconnected together.

The following are a few examples of networks in our everyday lives.

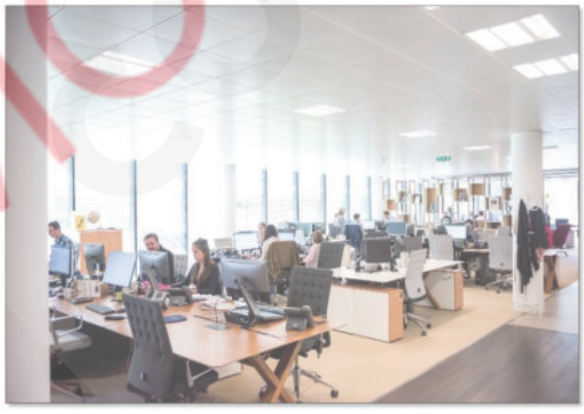
Social network

Mobile network

Airline network



Hospital network



Network of computers

Bank network

Figure 1.1.1: Networks

Computer networks

A **computer network** is an interconnection among two or more computers or computing devices. When the devices are connected, data and other resources, such as printers, computers, and laptops, are shared. The network is connected using **wires** like cables or **wireless** using WIFI.

For example, observe the computer lab at your school. This is a basic network that connects a few computers, printers, laptops in the lab. One printer in the lab can be shared with all through a network.

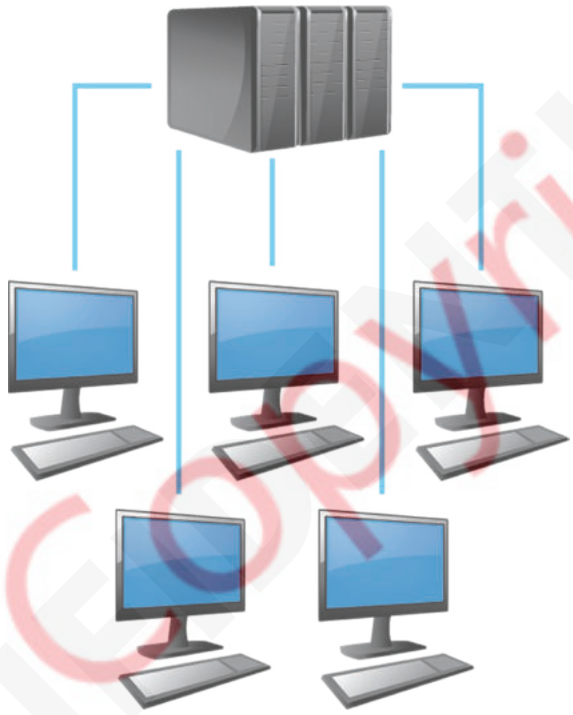


Figure 1.1.2: Computer networks

Types of networks

There are various types of computer networks. Some are connected wirelessly, while others are connected through wires. The connection is within a single room to the millions of computers spread across the globe. These networks are categorised based on the geographical area covered and data transfer rate from one device to another.

The different types of networks are:

- **PAN** (Personal Area Network)
- **LAN** (Local Area Network)
- **MAN** (Metropolitan Area Network)
- **WAN** (Wide Area Network)

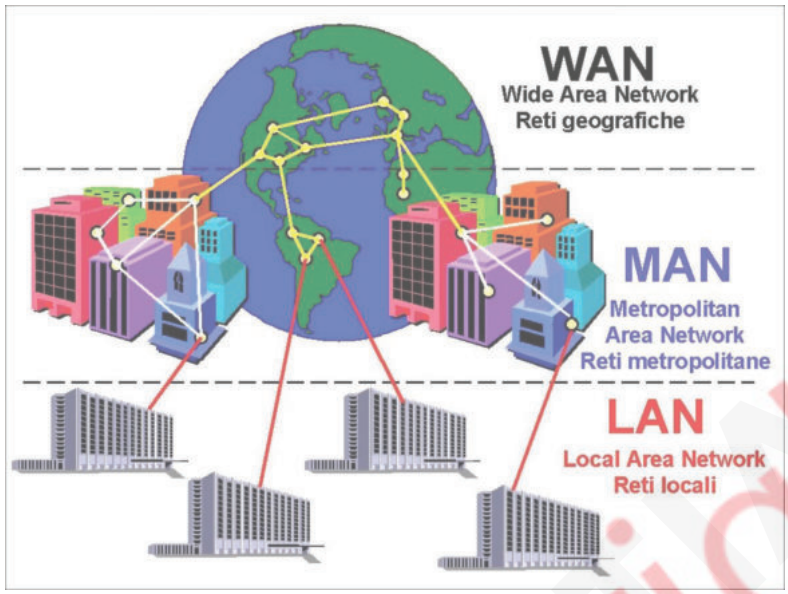


Figure 1.1.3: Types of computer networks

LAN (Local Area Network)

A local area network (LAN) is a network that is geographically limited to a single building or location. The organisation owns and maintains the LANs.

Examples include networks at schools, colleges, universities, small businesses, small organisations, and homes.

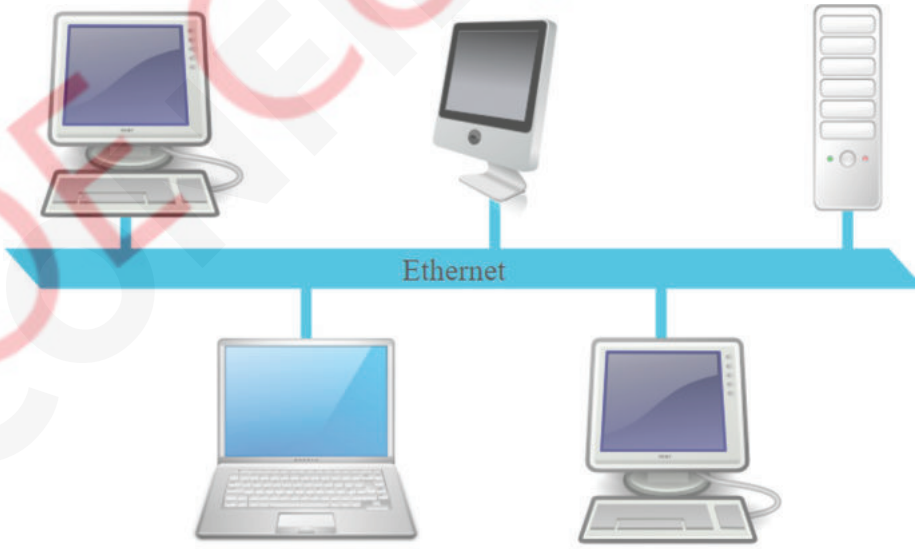


Figure 1.1.4: Local Area Network

WAN (Wide Area Network)

A wide area network (WAN) spreads over a wide geographical area. It can spread across a country or even the world. WAN connects more than one site.

Examples include banks, which are connected to more than one branch, using a WAN. The WAN connects the main headquarters to the sub-offices and branches, allowing them to communicate and share data. Telephone infrastructures or wireless transmission are used for communication. Each office or branch has its own LAN to which the WAN connects. Another example of a WAN connection is the **internet**.

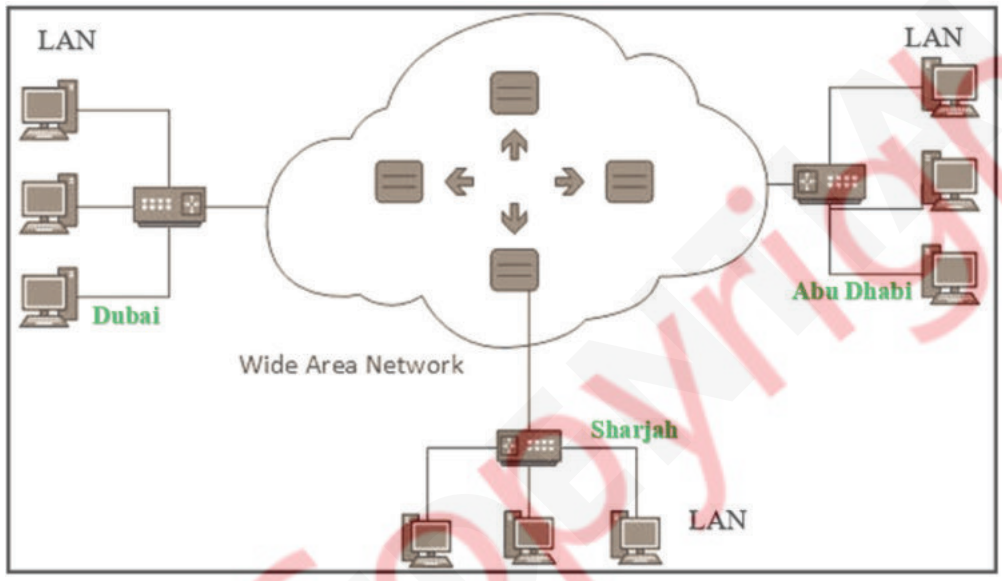


Figure 1.1.5: Wide Area Network

MAN (Metropolitan Area Network)

An extended form of LAN is the Metropolitan Area Network (MAN). It covers a larger geographical area like a city or a town.

Examples include cable TV networks or cable-based broadband internet services.

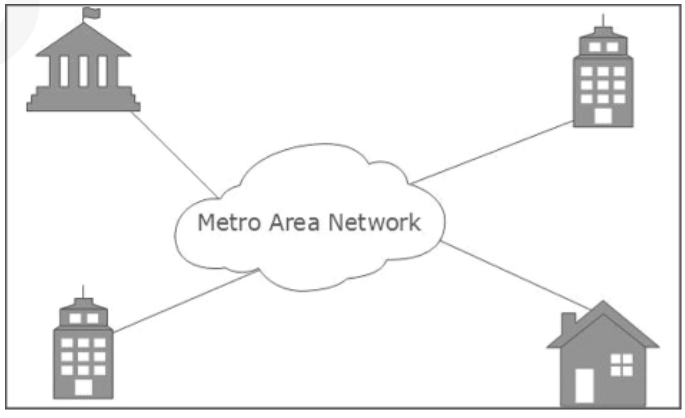


Figure 1.1.6: Metropolitan Area Network

PAN (Personal Area Network)

Personal devices like computers, laptops, mobile phones, smartphones, and printers are connected to form a Personal Area Network. A personal area network may be wired or wireless.

Examples of wired PAN include using USB to connect a mobile phone to a laptop. On the other hand, using Bluetooth technology to connect two smartphones is a form of a wireless PAN.

Figure 1.1.7: Personal Area Network

Complete activity 1.1.1 from the workbook

Network devices

Hardware devices that are used to connect computers, printers, laptops and other electronic devices to a network are called network devices. Different network devices are required to communicate data in a network. Let us explore a few of them.

MODEM

Modem stands for **MO**dulator and **DEM**odulator. It is used for conversion between analogue signals and digital bits.

- Analogue signals are continuous signals and are denoted by sine waves. The analogue signals use values that are in a continuous range. For example, for audio and video transmission, analogue signals are suited.

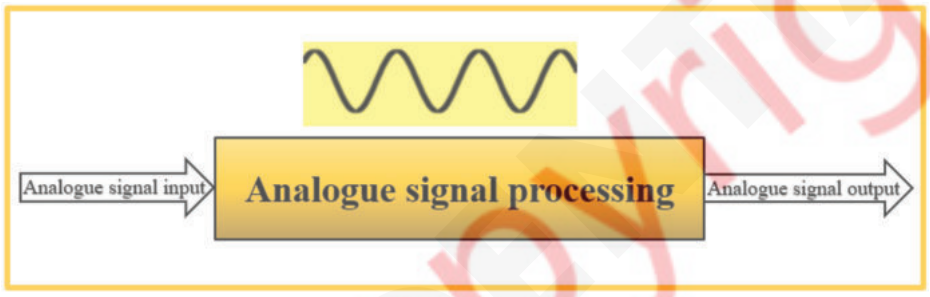


Figure 1.1.8: Analogue signal

- Digital signals are time separated signals and are denoted by square waves. Digital signals use only 0s and 1s to represent the information. For example, data transmission during computing and for digital electronics, digital signals are suited.

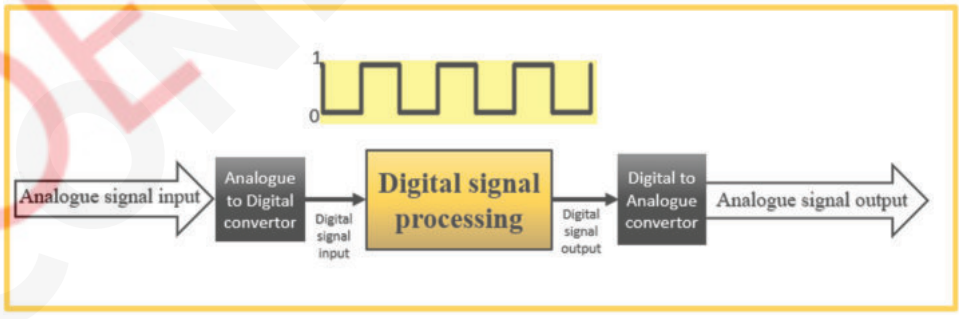


Figure 1.1.9: Digital signal

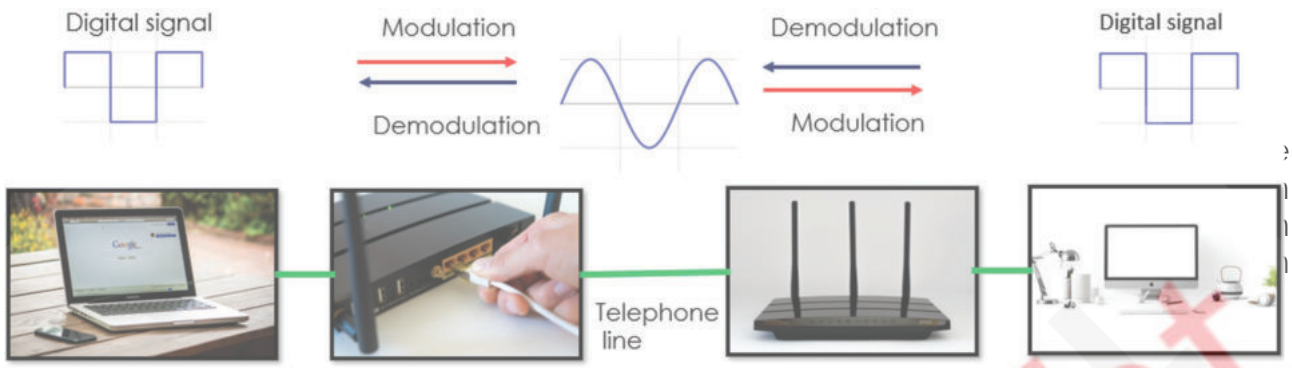


Figure 1.1.10: Modulation and Demodulation

The modem at the sender's end acts as a **modulator** that converts the digital data into analogue signals. The modem at the receiver's end acts as a **demodulator** that converts the analogue signals into digital data for the destination node to understand.

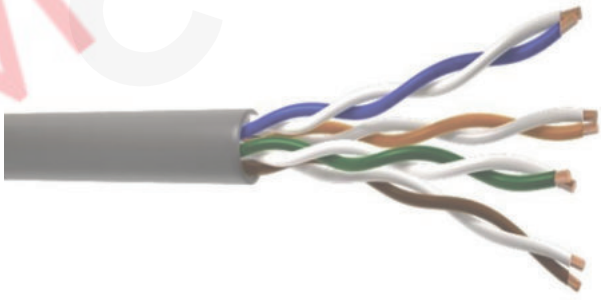
Network media

Network media are the communication channels in a network. It is the actual path over which an electrical signal travel. The signals move from one component to another. The common types of network media include twisted-pair cable, coaxial cable, fibre-optic cable, and wireless network.

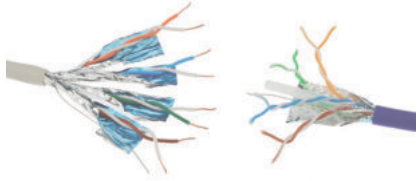
Twisted-pair cable

Twisted-pair cables are used for telephone communications and most modern Ethernet networks. For transmitting the data, a pair of wires are used to form a circuit. The pairs are twisted to provide protection against crosstalk, which is the noise generated by adjacent pairs.

Twisted-pair cables can be either STP (shielded twisted pair) or UTP (unshielded twisted pair). Their data transfer speed rate is between 10 to 1000 Mb/s, and the length is up to 100 meters.



UTP (unshielded twisted pair)

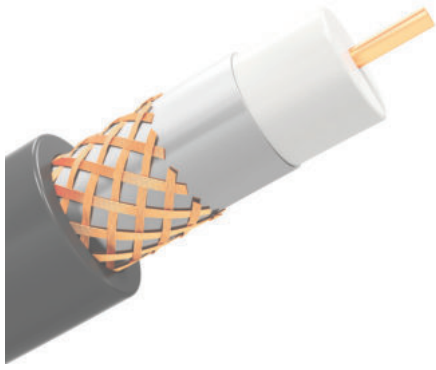


STP (shielded twisted pair)

Coaxial cable

Coaxial cable is a common type of shielded data transmission cable. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire made of two conducting elements. One of these elements, in the centre of the cable, is a copper conductor.

When using coaxial cables, the data transfer speed rate is between 10 to 100 Mbps. The length of the cable is up to 500 meters.



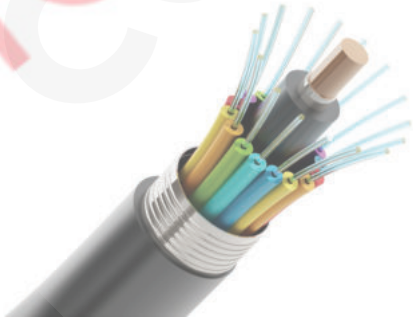
Coaxial cable

Coaxial cable connected

Fibre optics

Fibre optics cable is made up of 100 or more very thin strands of glass or plastic known as optical fibres. Each strand is capable of transmitting messages which turns into light waves.

The rate of data transfer speed of fibre optics cable is between 100 Mb/s to 1 Gb/s. Therefore, when fibre optics cable is used, the communication is much faster, especially over long distances.



Fibre optic cable structure

Fibre optics

Wireless networks

Wi-Fi networks do not use cables to connect and communicate with each other. Waves technology is used to communicate wirelessly between network devices. When there is a situation where cables cannot be extended, or networks do not prefer cables for communication, then wireless media can be used for sending and receiving data.

The different types of wave technologies for wireless communications are:

- Radio Frequency (RF) like Wi-Fi, 3G, 4G, 5G and Bluetooth
- Microwave
- Satellite
- Infrared

Wireless network

Wireless networks in a city

Ethernet card

Figure 1.1.11: Ethernet card

Ethernet card is also known as Network Interface Card (NIC). It is a piece of hardware that is used to set up a wired network. It acts as an interface or the joining place between the computer and the network. The ethernet cable is used to connect the computer to the network through NIC.

Figure 1.1.12: Ethernet cable

The network interface card (NIC)

The card or port where the network cable is connected is known as the network interface card (NIC). It changes the data from the computer into a signal that can be sent over the network medium, such as a copper cable. It also changes the signal it receives back into data that a computer can understand. Each NIC has a binary number called a Media Access Code (MAC) address. No two NICs in the world share the same MAC address. It is set when the NIC is made and cannot be changed. The MAC address identifies each device on a local network. It is used by computers to communicate on a local network.

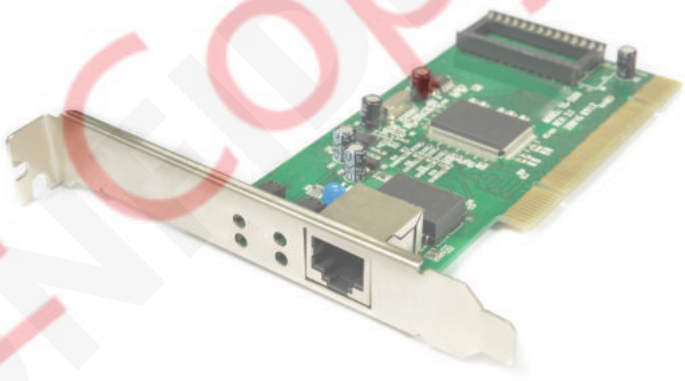


Figure 1.1.13: network interface card

Hub

A network device known as an ethernet hub is used in order to connect multiple computers on a single network through wires. A hub has a lot of lines or ports. It works as a central connection for all the devices connected. Data that comes in on one of them is sent out on all the others.

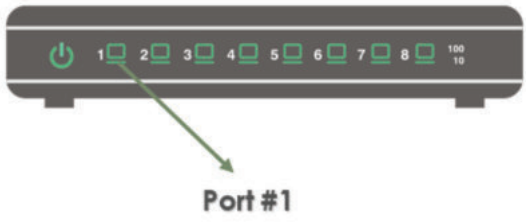


Figure 1.1.14: HUB

Switch

A switch is similar to an ethernet hub in that it has many ports to which computers can be connected. However, when data arrives, the switch examines the data and sends it to the correct device. At homes or offices, the ethernet switches are connected to multiple devices using cables. This connection creates LANs and also a way to access the internet.

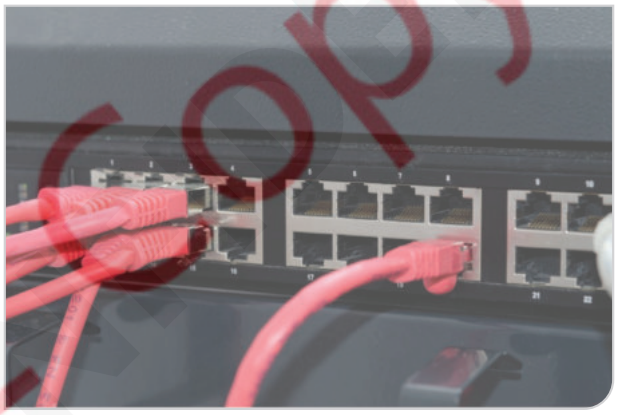


Figure 1.1.15: Switch

Router

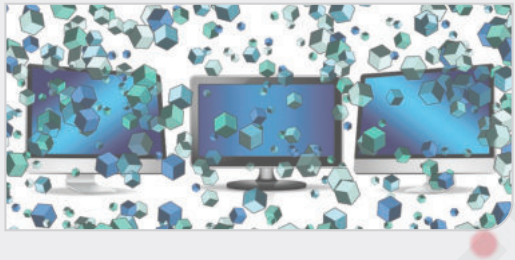
A router connects a local area network to the internet. There are two types of routers: wired and wireless. Smartphones and other devices can connect to the internet via a wireless router. Some ports on routers are used to give wired internet connection.

Modern Wi-Fi routers can function as both a router and a switch/modem. These routers link to incoming broadband lines from internet service providers (ISPs) such as Etisalat or DU in the United Arab Emirates. Then convert the data to digital data for computing devices to process.

When compared with a switch, a router is designed to do many other jobs. A router analyses the data over a network and checks the data packets. According to the data packet sizes, the router decides and sends the packet to another network of different type.

What is a packet?

A packet is a small portion of a large message in networking. Data is broken into packets and sent across computer networks. The computer or device that receives these packets then reassembles them.



For example, using internet, suppose a user needs to load an image. The image file does not go from a web server to the user's computer in one piece. Instead, it is broken down into packets of data and these packets are sent over the wires, cables, and radio waves of the internet. At the user's computer, these packets are reassembled to the original photo.

A router does the following task. Suppose data packets of a certain size are to be carried over a different type of network which cannot handle bigger packets. Then in this case, the data will be repackaged as smaller packets and then sent over the network by a router.

Figure 1.1.16: Router

Complete activity 1.1.2 from the workbook

Networking topologies

Computing devices are connected to form a network (LAN, WAN, MAN, PAN), and interconnections of many LAN networks form the internet. Network topology refers to the arrangement of computers and other peripherals in a network. The different types of network topologies include:

- Bus
- Star
- Ring
- Mesh
- Tree

Bus topology

In the bus topology, all devices are connected directly to a transmission medium called the bus. All signals pass through each of the devices. Therefore, a single backbone wire, the bus, is shared among the devices. Each device has a unique identity and can detect signals intended for its use.

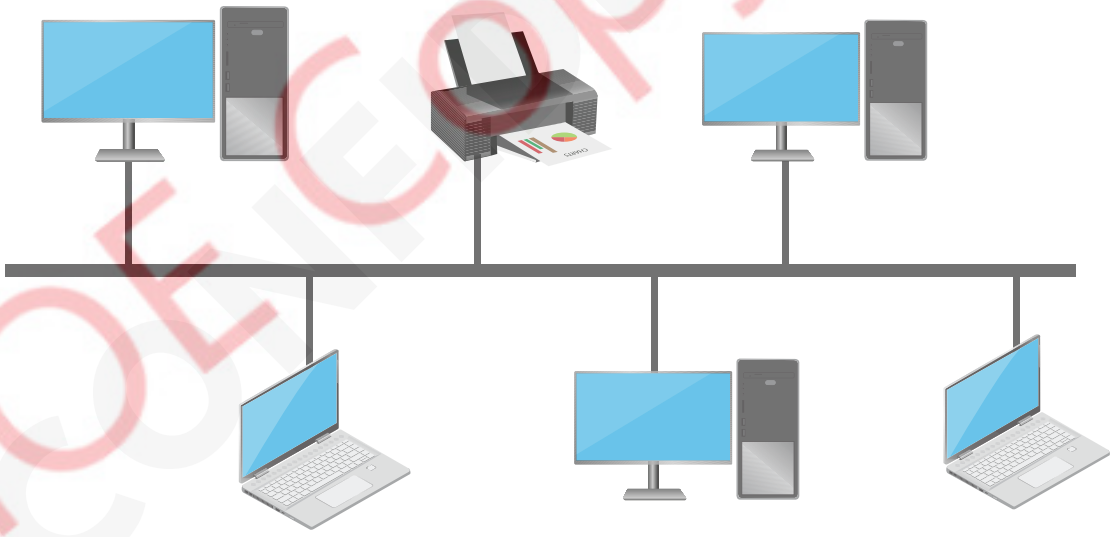


Figure 1.1.17: Bus topology

Star topology

In a star topology, each computer is individually wired to a central connecting device which can be a hub, switch, or router with twisted-pair cabling. It is one of the most common network setups.

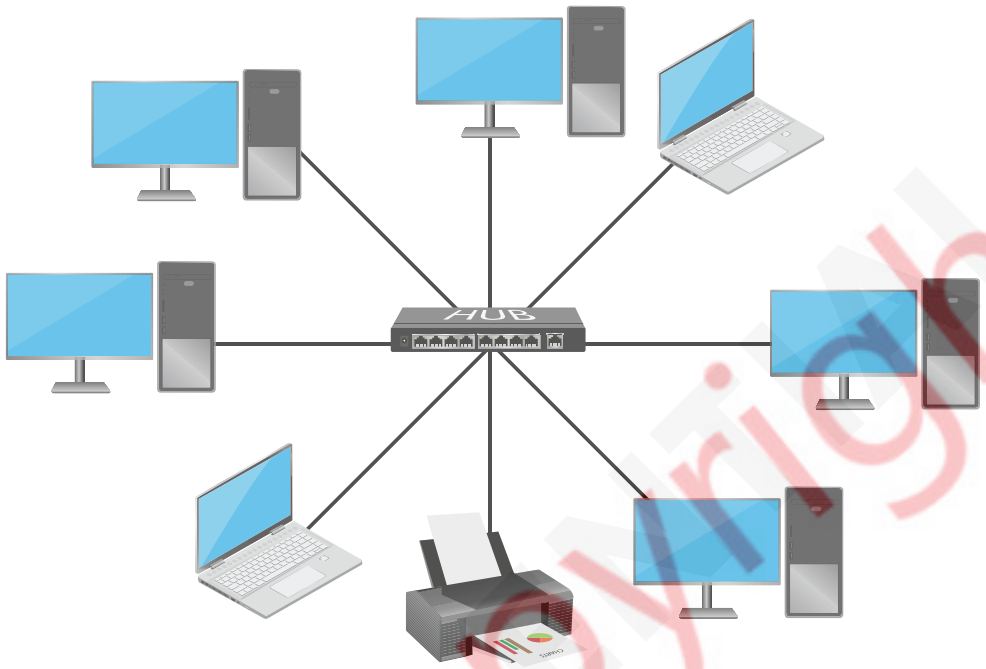


Figure 1.1.18: Star topology

Ring topology

In a ring topology, the devices are connected to each other in a circular shape. Each data packet is sent around the ring until it reaches its destination.

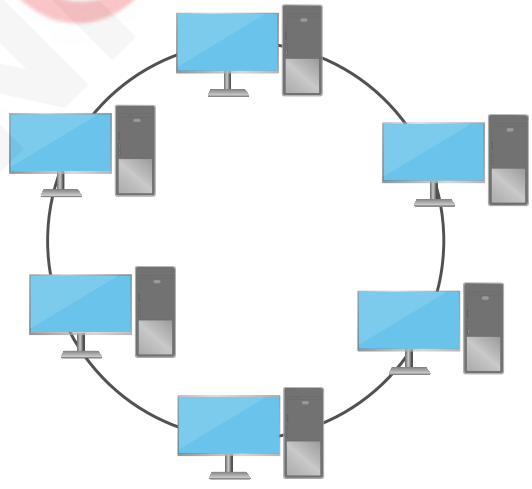


Figure 1.1.19: Ring topology

Mesh topology

In a mesh topology, each computer and network device is interconnected with every other device in the network. Each computer not only sends its own signals but also relays data from other computers.

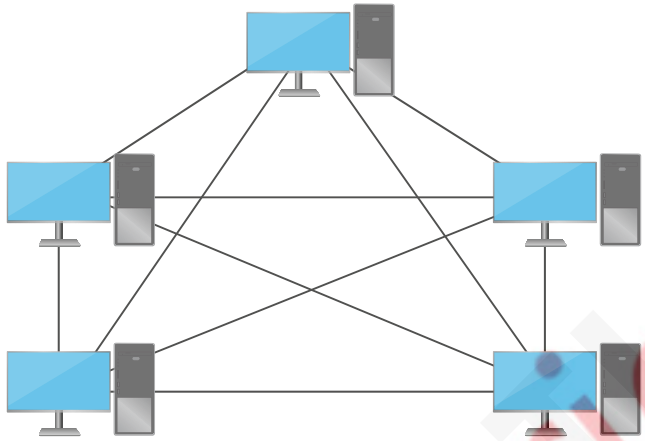


Figure 1.1.20: Ring topology

Tree or hybrid topology

In a hybrid topology, there are multiple branches. In each branch, there are one or more basic topologies like a star, ring, and bus. Hybrid topologies can be seen in a WAN where there are multiple LANs connected. The figure below shows a hybrid topology where a star and a ring network are connected.

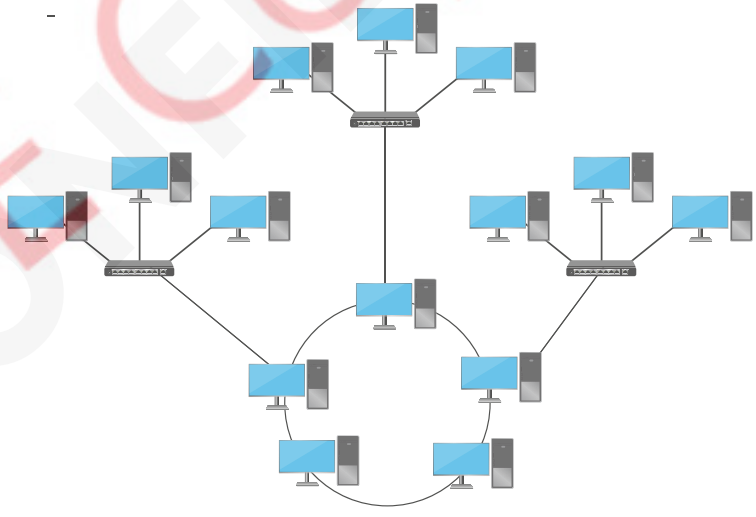


Figure 1.1.21: Ring topology

Complete activities 1.1.3 – 1.1.5 from the workbook

Network protocols

Computers and other devices communicate using a common language to understand the messages (or data) they receive over the network. This common language is called a **protocol**. There are many network protocols, including those listed below.

Ethernet

Ethernet protocols set out how data is arranged and transmitted over wired networks. Ethernet is the most common technology used for wired local area networks.

Figure 1.1.22: Ethernet

Internet Protocol (IP)

The Internet Protocol (IP) controls how data is sent between different networks. A computer using the Internet Protocol to communicate needs an IP address to send and receive data packets. An example of an IP address is 172.16.32.77. It provides the location of a computer on the internet. It is like a person's home address.

The Internet Protocol allows computers to send data packets to each device on the network.

MAC address

Each MAC address is a 12-digit hexadecimal number (48 bits in length). The first six digits (24 bits) is the device manufacturer's ID, also known as the Organisational Unique identifier (OUI). The next six digits (24 bits) represent the unique serial number assigned to the card by the manufacturer.

A sample MAC address is FC: C8: AE: CE: 5B:23. Here FC: C8: AE is the organisational unique identifier, and CE: 5B:23 is the unique serial number.

IP address

Internet Protocol (IP) address is a unique address that can be used to uniquely identify each device in a network. If a computer's IP address is known, then that computer can be communicated from anywhere in the world. However, unlike MAC address, IP address changes if the network is changed.

IPV4

The initial IP address, version 4 (IPV4), is a 32-bit numeric address. The IP address is written as four 8-bit decimal numbers separated by periods. Each 8-bit field can take any value from 0 - 255.

An example of an IPV4 address is **192.168.112.231**

IPV6

Due to the increasing number of devices connected to the internet, the 32-bit IP address **(IPV4)** was no longer sufficient, as it can offer less than a billion unique addresses. Therefore, a 128 bits IP address, known as IP version 6 **(IPV6)** was introduced. An IPV6 address is represented by eight groups of hexadecimal (base-16) numbers separated by colons.

An example of a IPV6 address is **2001:0db8:85a3:0000:0000:8a2e: 0370:7334**

Figure 1.1.23: IPv4 and IPv6

Complete activity 1.1.6 from the 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. .....

Key skills reflection

Learning outcomes	Key Skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand.	I'm an expert
Explain the relationship between routers, switches, servers, topology, protocols and addressing.	I can explain routers, switches, servers, topology, protocols and addressing.			
	I can explain the relationship between routers, switches, servers, topology, protocols and addressing.			
Implement networks using a range of hardware, topologies, protocols and addressing.	I can illustrate networks using a range of hardware and topologies.			
	I can implement networks using a range of hardware, topologies, protocols and addressing.			
Teacher's comment:				

Section 2: Network security

Aim

In section 2, you will learn about the cybersecurity measures that can be used to protect a computer network from cyber-attacks. You will explore them in terms of usability and security. Next, you will learn how data can be affected by malware and other attacks.

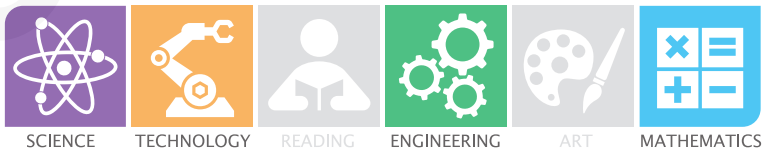
Learning outcomes

- Explain a range of security measures and how they impact the usability and security of a computing system.
- Illustrate how examples of sensitive data can be affected by malware and other attacks.
- Implement a range of cybersecurity measures in a computer system.
- Select a range of appropriate cybersecurity measures for implementation in a computer system.

Prior knowledge

- Computer science

My STREAM focus



Key vocabulary

WORD	MEANING	PICTURE
network security	practice of taking precautions to safeguard the underlying networking infrastructure against the attackers	
malware	software that is designed to damage and destroy computer systems	
usability	degree to which something is able or fit to be used	
sensitive data	private information that must be kept secure	
cybersecurity	practice of protecting systems, networks, and programs from digital attacks	

What is network security?

Network security is important for both home and business networks. The internet is used everywhere, and wireless routers are becoming more common. Some people try to harm internet-connected computers, invade people's privacy, and prevent them from using internet services. Therefore, if the network is not protected, there may be data loss, theft, or damage.

Figure 1.2.1: Network security

Network security is the practice of taking precautions to safeguard the underlying networking infrastructure against the following:

- Illegal access
- Misuse
- Malfunction
- Alteration
- Destruction, or improper disclosure

Network security mechanisms

Network security has become a central concern today due to the frequency and variety of existing and more damaging future attacks. Computers, users, and programs can execute their permitted important tasks in a secure environment by implementing network security mechanisms.

To protect the network, the following measures are taken:

- Firewalls
- Password management
- Access control
- Anti-malware software
- Application security
- Virtual Private Network (VPN)
- Email security
- Mobile device security

Firewalls

A firewall is software or hardware designed to block unauthorised access to computers and networks. The firewall is designed with a series of rules. Therefore, the incoming and outgoing network traffic is controlled by these firewall rules. Computers and networks that follow the firewall rules are allowed access points, as shown in the figure below. If the rules are not followed, then the firewall prevents accessing the computers and the networks.

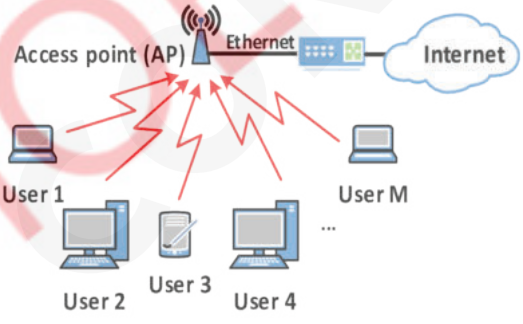


Figure 1.2.2: Access points

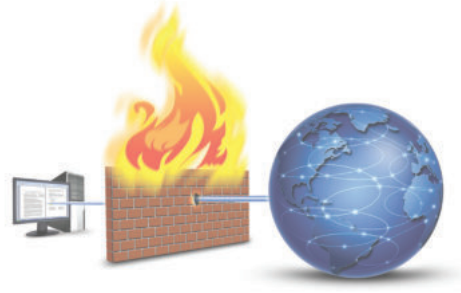


Figure 1.2.3: Firewall

Password management

Using unique and strong passwords makes it difficult for hackers to gain access to your network. Avoid common passwords or phrases like 'password', '12345', date of birth or names. For added security, use passwords that feature a combination of letters, symbols, numbers, and uppercase letters. It is recommended to regularly change any personal passwords used on systems with access to business networks.

Figure 1.2.4: Weak password

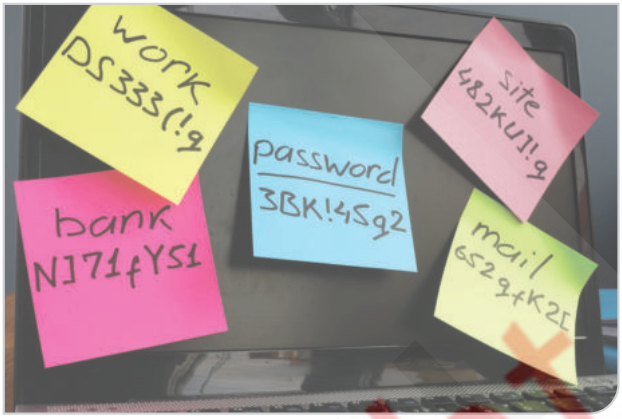


Figure 1.2.5: Strong passwords

Access control

Network Access Control (NAC) is security software application that restricts the number and types of users who have access to a network. Not all users require access to the network. Therefore, to prevent hackers from gaining access, the access control centre keeps track of each user and device and decide which ones are permitted in. Network access control can also set security policies and parameters.

Figure 1.2.6:Access control

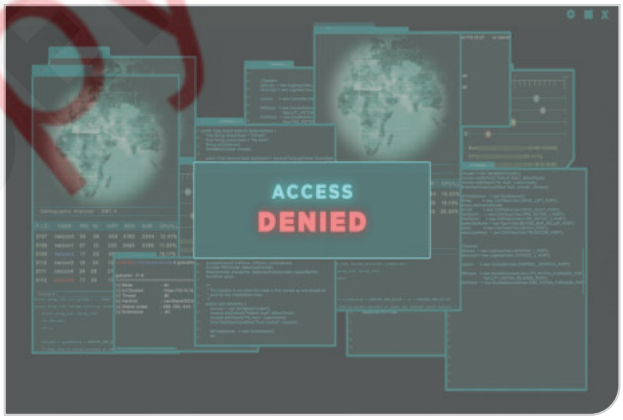


Figure 1.2.7: Access denied

Anti-malware software

Malware are known as 'malicious software'. This software can be a worm, virus, spyware, trojan, or ransomware.

Table 1.2.1: Types of Malware

Malware	Description
Virus	Malicious software that is attached to a document or file and spreads from system to system.
Worms	Malicious software that replicates and spreads to any device within the network.
Spyware	Malicious software that runs secretly on a computer and reports back to a remote user.
Trojan	A virus that gains access to sensitive data and then modifies, blocks, or deletes the data.
Ransomware	Malicious software that gains access to sensitive information within a system and changes that information so that the user cannot access it. Then it demands a financial payout from the user for the data to be released.

If a network is infected with malware, the bug may remain hidden in the network for weeks. A malware attack could occur at any moment and affect the network without warning.

To prevent the malware attack, **antivirus/anti-malware software** is designed to detect the malware. Antivirus software scans for the viruses and blocks them from entering your network.

Figure 1.2.8: Malware

Application security

Application security refers to security precautions implemented at the application level to prevent the loss or theft of data or code within the app. During the design and development of applications, security concerns, methods, and other design elements must be taken into account.

User authentication-authorization

Figure 1.2.9: Authentication and authorisation

Authentication and **authorisation** are common types of application security.

Authentication is a process to ensure only authorised users gain access to the application. Software developers must use security technologies such as identity authentication to make sure that the users are who they claim to be. Authentication can be performed by comparing the user's identification with a list of authorised users, ensuring the user has permission to access the program/application.

Once a user has been authenticated, the user may be **authorised**/permitted to access and use the application.

Virtual Private Network (VPN)

During COVID 19 pandemic, remote working has increased significantly which means more people are online. This has increased their exposure to cybercrime, making them more vulnerable. Virtual Private Network (VPN) is created to secure the connection between remote computers and other computers. For example, users working from home can connect to the organisation's network over a VPN.

VPN is available only to authorised people who have access to the network and devices. VPN increases network security by not allowing unauthorised people to enter the system.

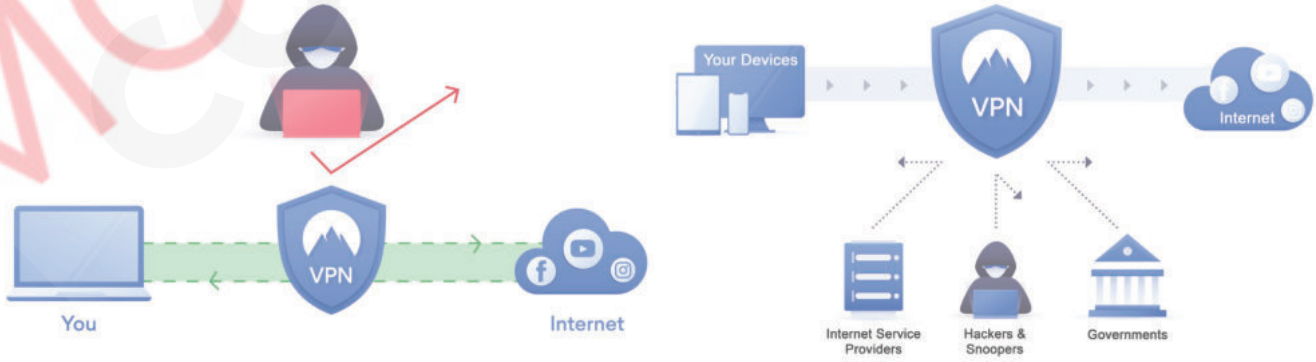


Figure 1.2.10: Virtual Point Network (VPN)

Email security

Phishing is a technique where suspicious emails are sent to users to trick them into falling for a scam. Hackers can easily gain access to users' personal information, mislead them, and send them to sites that contain malware. With **email security software**, the network is protected as the software blocks incoming attacks and have control over outbound messages.

Figure 1.2.11: Email scam

Mobile device security

Mobile devices are electronic devices with portable functionality. Example of mobile devices include smartphones, tablets, laptops, smartwatches, e-readers, and handheld gaming consoles.

The attackers can easily gain access to the network by targeting the users' mobile devices through the applications they have downloaded. Users must have control over which mobile devices can access the network and configure their connections to keep the network traffic private. Therefore, to protect your devices from attackers, it is important to turn off Bluetooth, avoid using unsecured public Wi-Fi networks, and create complex passwords.

Figure 1.2.12: Mobile device security

Complete activities 1.2.1 and 1.2.2 from the workbook

What is usability?

Usability refers to how well a certain user in a specific situation can use a product/design to accomplish a defined goal effectively, efficiently, and successfully.

Figure 1.2.13: Usability and security

Did you know?

"Usability is about human behaviour. It recognises that humans are lazy, get emotional, are not interested in putting a lot of effort into, say, getting a credit card and generally prefer things that are easy to do vs. those that are hard to do."

— David McQuillen, ex-Swiss banker and founder of Sufferfest cycling workout resources

Security versus usability

Usability is about more than just ease of use. It is also about user satisfaction, which can be achieved through engaging content, visually appealing design, and effective functionality.

Security features and techniques are designed to be utilised effectively. Human thinking plays a major role here. People want security as a goal, but in practice, people feel that more security means less usability. In general, for systems and services to be truly secure, they must have good security features with easy configuration and usage.

It is not easy to have great usability and good security at the same time. The following example, forgot password, explains the impact of security measures in terms of usability and security.

Forgot password

There have been many attempts to solve security issues without truly considering human usability, like passwords.

- In 2017, the average business user had 191 password-protected accounts. Without reusing passwords or using a password management service, this is impossible.

Security: To avoid reusing the same password, the security community recommends changing passwords on a regular basis and making them only valid for a certain amount of time.

Usability: This resulted in people using extremely predictable passwords, making it easier for hackers to steal the data.

- As a result, multi-factor authentication (MFA) was introduced. MFA can be seen in apps like Google authenticator.

Security: Multi-factor Authentication (MFA) is an authentication method where a user provides two or more verification factors to gain access to a resource (application, phone, laptop). An example for MFA is shown in the figure below.

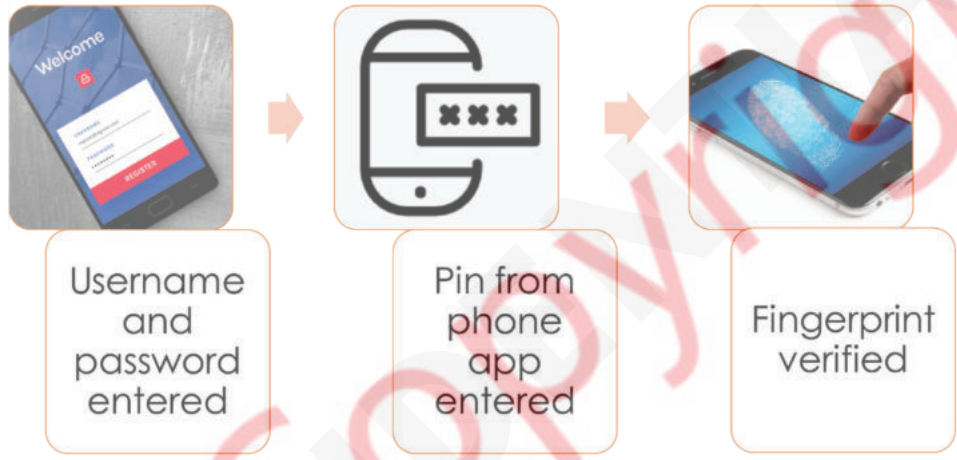


Figure 1.2.14: Multi-factor Authentication (MFA)

Usability: Even after MFA was implemented, there were still certain risks that this method was unable to address. For example, from a security point of view, the following questions posed some challenges.

- What is the users' location when trying to access the information?
- Is the user accessing the company's information during normal working hours or during 'off hours'?
- Is the device (laptop/mobile) used the same as what was used yesterday?
- Is the connection established over a private network or a public network?

MFA has been introduced to users in recent years. In 2016, less than 10 per cent of Google accounts users only used MFA.

- The next invention was the Universal 2nd Factor (U2F). This was a great advancement in both usability and security. With the Yubikey nano and other U2F devices, the user need to use another registered device or use the physical key to authenticate, which increases the security.

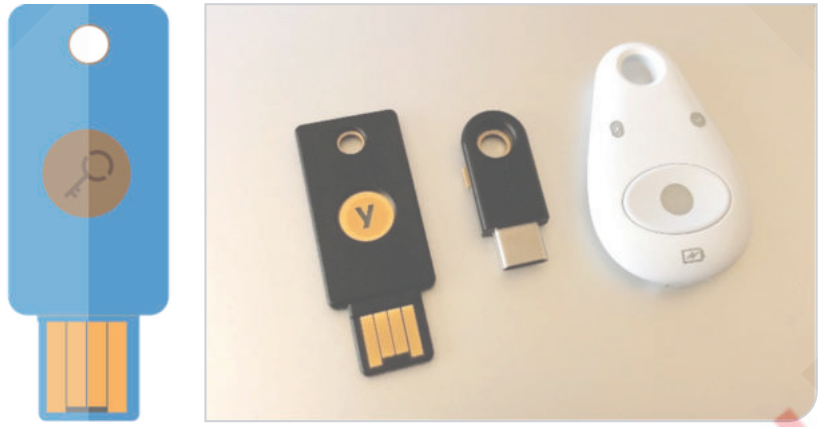


Figure 1.2.15: Yubikey

Figure 1.2.16: Universal 2nd Factor (U2F)

Security: U2F has strong defences against phishing , and it is easy to use.

Usability: U2F requires purchasing a separate device (Yubikey). Since purchasing a device is an additional task and cost to users, this method went down and became a rare use among users.

Therefore, in the above-mentioned methods, MFA was quite an additional job for users, so mostly they do not want to use MFA. But this situation has changed in recent years. For example, in mobile devices, when the users were asked to enter a password or pin for security, the users avoided it because entering a password or pin prevented the users from using the phone. Mobile users unlock their smartphones about 80 times per day on average.

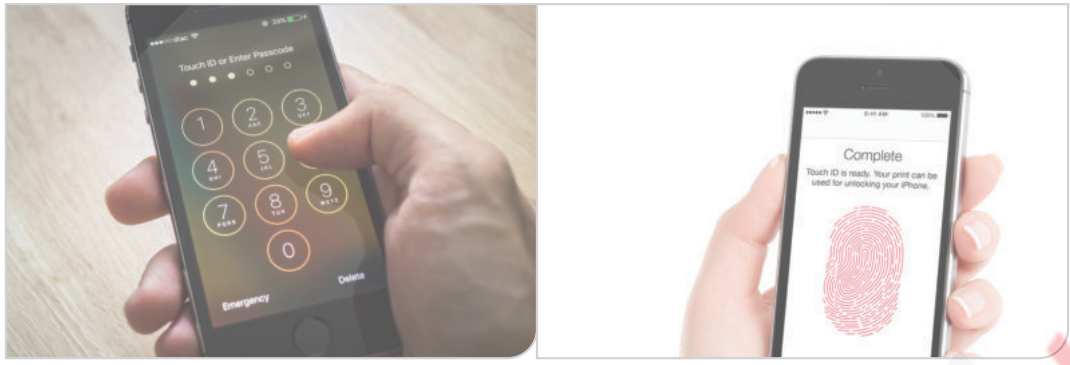


Figure 1.2.17: Passcode and fingerprint

Following technological advancements, Apple added the touch ID and Face ID features to its iPhones. In addition to these features, biometric configurations such as voice recognition, fingerprint scanning, and facial recognition were added to the phone setup. Now due to this additional features, around 90% of users have enabled screen lock on their smartphones. Therefore, security technology must be easy to use.

A few years ago, there was always a situation where security was compromised if the user required usability, and usability was compromised if the user required security. However, things have changed lately in modern technology. Security and usable functionality are built together with significant advancements in modern technologies and solutions.

Sensitive data

Sensitive data is private information that must be kept secure and out of the hands of anyone who does not have permission or authorisation to see it.

Data security measures should be in place to limit the hackers from accessing sensitive data and protecting the data from malware attacks. Personal information and business information are the types of sensitive data that hackers tend to exploit.

Sensitive data in individual, private or government organisations can be classified into four types:

- Low data sensitivity
- Moderate data sensitivity
- High/confidential data sensitivity
- Restricted type of sensitive data

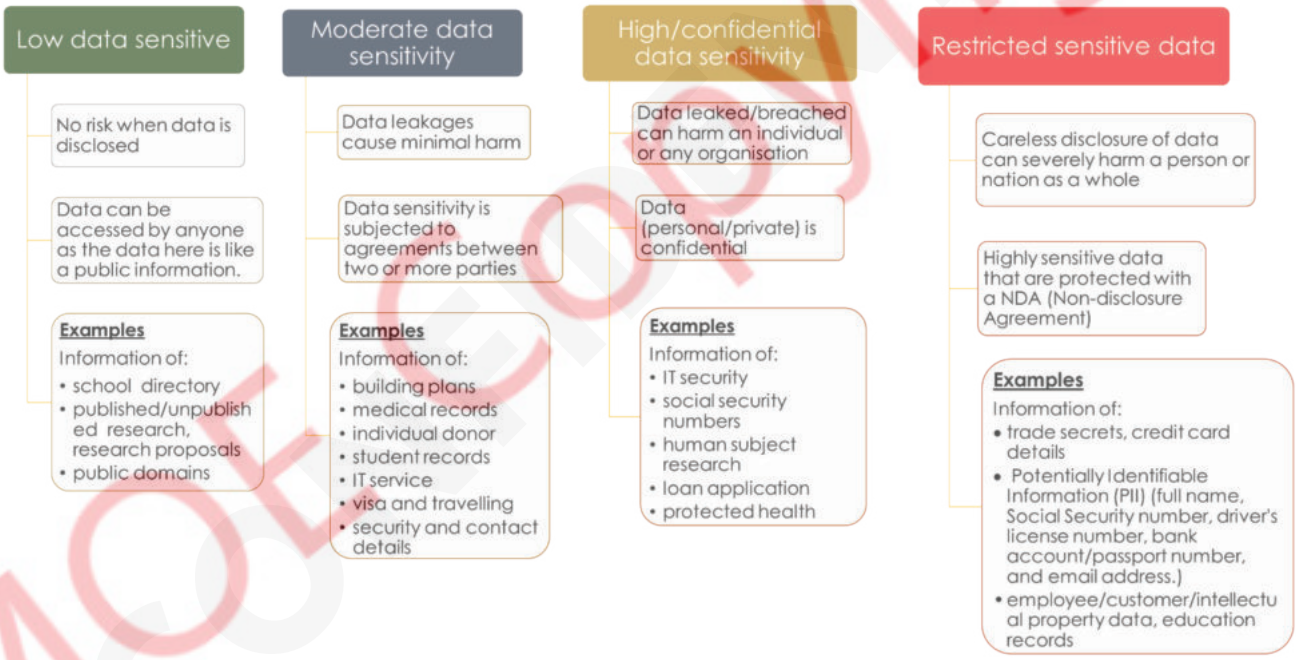


Figure 1.2.18: Sensitive data

Malware and the sensitive data

Malware, often known as malicious software, is a type of program that can harm a computer and its network. It is used by hackers to steal passwords, erase files, and disable computers. A malware attack can cause plenty of issues that affect the **business's** day-to-day operation as well as its long-term security.

Here are a few things that malware attacks can do.

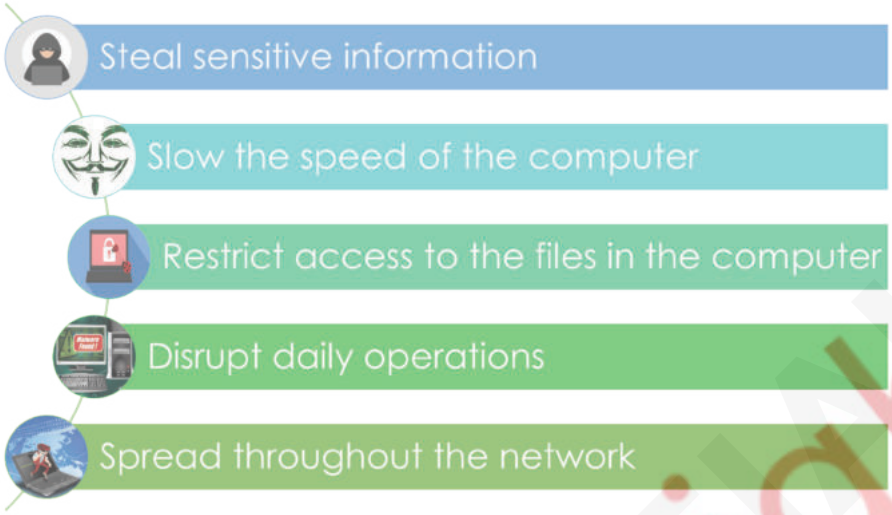


Figure 1.2.19: Result of malware attack

How to prevent malware attacks?

The following steps can minimise the risk of malware threats.

Install anti-malware software

Anti-virus software and other anti-malware programs can identify and remove many types of malwares. Using this software, performing regular checks is good to improve the network.

Security training

Security training encourages employees to understand IT security issues, identify security risks, and learn the importance of responding to security issues. Data gets hacked mostly due to employee error. Regular network safety trainings are strongly suggested for increasing security.

Avoid clicking unknown links and pop-ups

Pop-ups and files are frequently infected with malware, which is eventually installed on the system. It is suggested that only expected files from trusted sources be opened. Before clicking on a link, it is also necessary to look at it.

Update the system regularly

Every day, a million new malware threats are created. As a result, it is important to keep the system as current as possible. It is recommended to check operating system and anti-virus for new updates and install them on a regular basis.

Implement network security

It is important to keep track on the IT systems on a regular basis to protect the data from hackers. This management can be done within the company or by using a service from other company.

Complete activities 1.2.3 – 1.2.6 in the workbook

Cybersecurity

Now that you know about network security, it is time to explore cybersecurity. So, what exactly is cybersecurity?

Figure 1.2.20

Cybersecurity is all about protecting our computer systems, networks, and data from digital attacks. The people who carry out these attacks are known as cybercriminals or hackers. These digital attackers steal, alter, or destroy important information. Their actions can lead to financial losses or cause disturbances in doing regular work or activities. That is why it is important to understand and practice cybersecurity to keep ourselves safe online.

Cybersecurity measures

Cyberspace is anything that has to do with the Internet. Some common online issues children face in their digital lives include:

- **cyber predators,** where people use the internet to try and trick or harm internet users.
- **cyberbullying,** where people use technology, such as the internet, social media, or phones, to hurt others.
- **identity theft,** where someone steals another person's personal information and pretends to be that person.

Figure 1.2.21

Cybersecurity measures are a set of actions, practices, and technologies implemented to protect computer systems, networks, data, and users from cyber-attacks. A list of cybersecurity measures to be taken to protect from cyberattacks is shown below.

Figure 1.2.22

Complete activity 1.2.7 and lab activity 1.2.1 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. .....

Key skills reflection

Learning outcomes	Key Skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand.	I'm an expert
Analyse the sustainable benefits of emerging enabling technologies.	I can explain a range of security measures that can be used to protect a network.			
	I can explain the impact in terms of usability and security for a range of security measures used to protect a network.			
Illustrate how examples of sensitive data can be affected by malware and other attacks.	I can explain how examples of sensitive data can be affected by malware and other attacks.			
	I can illustrate how examples of sensitive data can be affected by malware and other attacks.			

MOEUAEofficial