Year 7
Computer Science 7.2

Malicious soft**ware** created to harm or gain illegal access to computer systems.

A **virus** is a type of malware which spreads by attaching itself to files. The virus then causes the computer system to **malfunction** in some way.

Scareware is a type of malware that creates false messages to trick the user into following **malicious** links.

Ransomware is a type of malware that uses **encryption** to lock the user out of their files then requests a large sum of money to **decrypt** and return the data

Spyware is a type of malware which monitors and records user actions.

A **rootkit** is a set of software tools that enable an unauthorised user to gain control of a computer system without being detected.

A **Trojan** is a type of malware which is disguised as legitimate software.

Symptoms of an infected computer:

1. Unexpected pop-up windows
2. Slow start up and slow performance
3. Lack of storage space
4. Missing files
5. Crashes and error messages

Social Engineering is a way of gathering sensitive information or illegal access to networks by tricking / manipulating people.

Phishing is the sending of emails or text messages claiming or appearing to be from a bank/ e-commerce site asking for personal details and/or credit card details.

Shouldering involves finding passwords and pins by watching people enter them.
This could happen in a busy office or at a distance using binoculars or recording equipment.

Blagging involves a criminal inventing a scenario to persuade a victim to give out information.
e.g. they could pretend to be another employee/technician.

A **network** is 2 or more devices connected to share data.

A Local area network (**LAN**) is 2 or more devices connected in a small geographical area (usually in one building).

A Wide area network (**WAN**) is 2 or more LAN's connected (via the internet) over a large geographical area.

Networks are created to allow the sharing of:

- ✓ Data
- ✓ Hardware (printers etc.)
- ✓ Internet connection

A network attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without *authorised* access.

A **passive attack** is where a hacker intercepts data travelling on a network usually using packet sniffers.

An **active attack** is where someone attacks a network with malware.

An **insider attack** is where someone inside the organisation EXPLOITS their network access to steal information

A **brute force attack** involves gaining information / access to a network through cracking passwords.
Brute force attacks use automated software which produces hundreds of likely passwords.

Increasing the **security** of a computer system of network can be done by:

- ✓ *Installing up to date anti-malware*
- ✓ *Using strong passwords*
- ✓ *Using anti-spyware software*
- ✓ *Not opening attachments from suspicious emails.*
- ✓ *Being careful when downloading files from the internet.*
- ✓ *Installing and using a firewall.*

Password requirements:

- ✓ At least one lower case letter [a-z]
- ✓ At least one upper case letter [A-Z]
- At least one numeral [0-9]
- At least one symbol [!@#^&*()+_,.{}?-]
- Minimum 8 characters
- ✓ Maximum 20 characters

Tier 2

malicious, malfunction, unauthorised, detected, disguised, legitimate, manipulating, e-commerce, scenario, persuade, obtain, alter, destroy, remove, implant, reveal, authorised, exploit

Year 7 Computer Science - Topic 7.2 System Security

What I need to know:

Define malware			
List 5 types of malware.			
Explain what a virus is / does.			
Explain what scareware is/ does.			
Explain what ransomware is/ does.			
Explain what spyware is / does.			
Explain what a rootkit is / does.			
Explain what a Trojan is / does.			
List the symptoms of an infected computer system.			
Define social engineering.			
Explain how phishing works.			
Explain how shouldering works.			
Explain how blagging works.			
Define the term network.			
What do LAN and WAN stand for?			
Define LAN and WAN.			
Give 3 reasons for creating a network.			
What is a network attack?			
Describe a passive attack.			
Describe an active attack.			
Describe an insider attack.			
Describe a brute force attack.			
Describe 3 ways in which security can be increased on a computer system/network.			
What advice would you give someone who wants to create a strong password.			