GCSE Computer Science
Topic 1.6 System Security (1)

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

Network attacks bypass users and attack the network operating system and security:

PASSIVE ATTACK: hackers monitor the data travelling on a network and intercept any sensitive information they find (login details, passwords, credit card details etc.).
They use network-monitoring tools such as packet sniffers.
DEFENSE: ENCRYPTION

ACTIVE ATTACK: A network attack performed using malware.
MALWARE is designed to disrupt the function of a computer or collect information.
DEFENSE: FIREWALL /ANTIVIRUS SOFTWARE

INSIDER ATTACK: this is where someone inside the organisation EXPLOITS their network access to steal information.
DEFENSE: USER ACCESS LEVELS

BRUTE FORCE: involves gaining information / access to a network through cracking passwords.
Brute force attacks use automated software which produces hundreds of likely passwords.
DEFENSE: SECURE PASSWORDS/ LOCKING ACCOUNTS

DOS attacks overload a network or website by flooding it with network communications such as login requests. (Making the network/website extremely slow or unavailable).
DEFENSE: FIREWALLS

Many forms of attack target USERS by getting them to install MALWARE (harmful software) on their computers, which cause damage to / disrupt systems in different ways:

MALicious soft**WARE**
Is software that can harm devices.
It is installed on someone's device without their knowledge or consent.

SCAREWARE : malware that tells the user that their device is infected with lots of viruses.
It scares them into clicking on MALICIOUS links or paying for fictional problems to be fixed.

RANSOMWARE: malware which locks/ encrypts files.
The user receives a message demanding a large sum of money for the decryption key.

SPYWARE malware which stays hidden / out of view and is designed to spy on your computer, looking for personal information, passwords etc.

It does this by using a key logger to record every key pressed on the keyboard. It might also take screen shots. This information is then sent secretly over the internet to the criminals.

ROOTKITS are malware which give other people admin-permissions and access to your computer, allowing them to take it over remotely and do whatever they like.

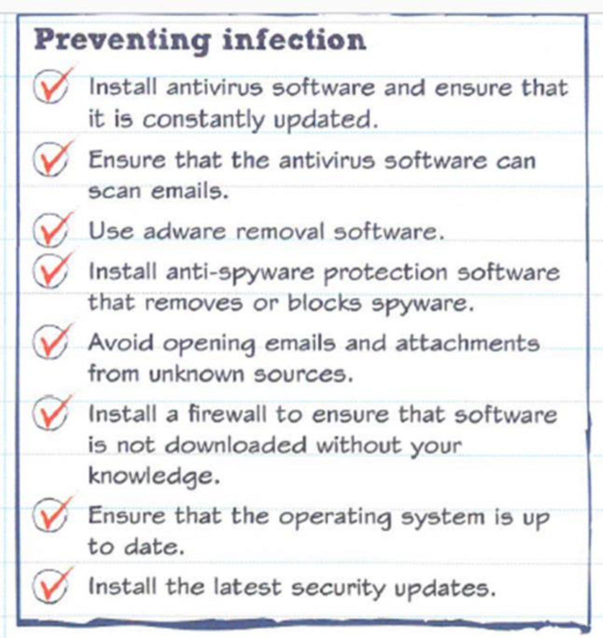
It is designed to run even before the operating system itself is booted up and it continues to stay active in the background while you are using the computer.

VIRUSES: malware which attaches (by copying themselves) to certain files. E.g. .exe files

When users open the files they activate them, then the viruses spread onto other files on their system.

WORMS: malware. like viruses, but they SELF REPLICATE without any user help.
They spread very quickly.

TROJANS: malware that is disguised as legitimate software.
They don't replicate themselves, users install them, not realising they have a hidden purpose.



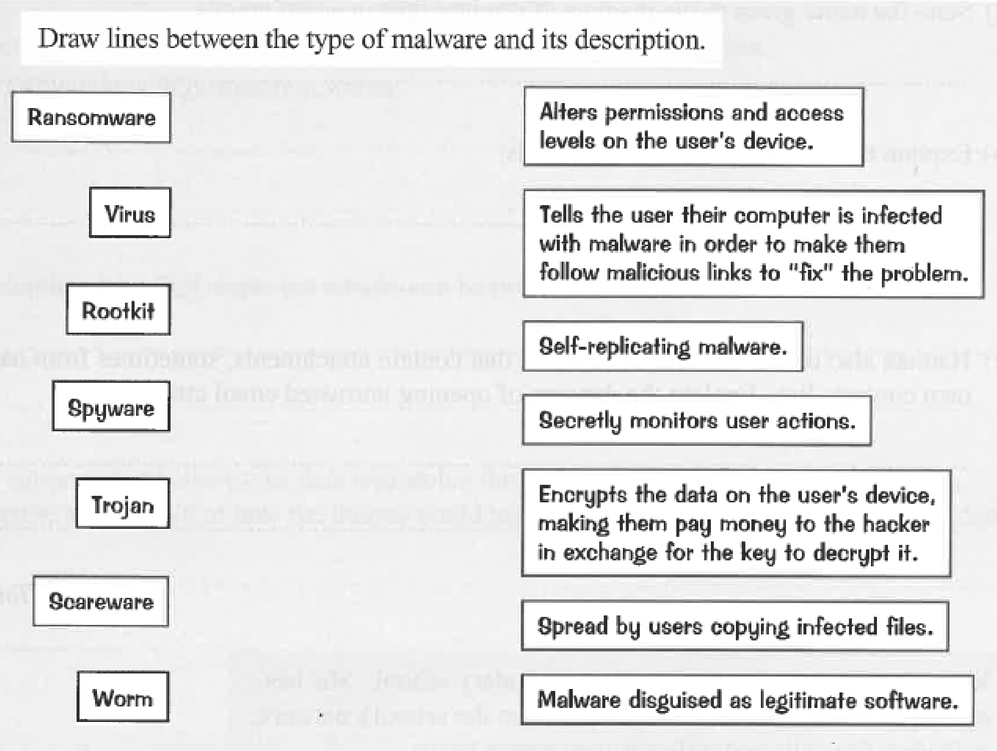
Preventing infection

- ✓ Install antivirus software and ensure that it is constantly updated.
- ✓ Ensure that the antivirus software can scan emails.
- ✓ Use adware removal software.
- ✓ Install anti-spyware protection software that removes or blocks spyware.
- ✓ Avoid opening emails and attachments from unknown sources.
- ✓ Install a firewall to ensure that software is not downloaded without your knowledge.
- ✓ Ensure that the operating system is up to date.
- ✓ Install the latest security updates.

GCSE Computer Science - Topic 1.6 System Security (1)

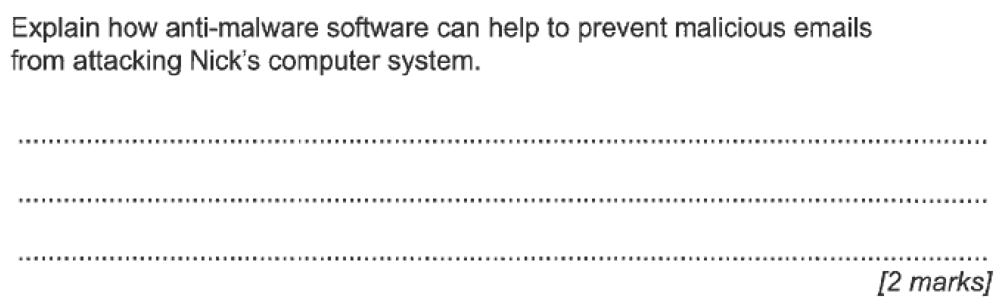
What I need to know:

Describe what is meant by an attack.
Describe how a network attack works.
State the name of the 5 main forms of NETWORK attack.
Describe a passive NETWORK attack.
Describe an active NETWORK attack.
Describe an insider NETWORK attack.
Describe a brute force NETWORK attack.
Describe a DOS NETWORK attack .
Define malware.
Describe how a malware attack works.
Describe scareware.
Describe ransomware.
Describe spyware.
Describe rootkit malware.
Describe virus malware.
Describe worm malware.
Describe Trojan horse malware.
Describe some actions that can be taken to protect against the infection of malware.



Draw lines between the type of malware and its description.

Ransomware	Alters permissions and access levels on the user's device.
Virus	Tells the user their computer is infected with malware in order to make them follow malicious links to "fix" the problem.
Rootkit	Self-replicating malware.
Spyware	Secretly monitors user actions.
Trojan	Encrypts the data on the user's device, making them pay money to the hacker in exchange for the key to decrypt it.
Scareware	Spread by users copying infected files.
Worm	Malware disguised as legitimate software.



Explain how anti-malware software can help to prevent malicious emails from attacking Nick's computer system.

....

....

....

[2 marks]