Paper 1 | GCSE Computer Science | 1.4 Network Security Revision Sheet

Social Engineering
A way of gaining sensitive information or illegal access to networks by influencing people, often takes place **over the telephone or phishing**.

A good network policy will regularly test the network to find and fix security weaknesses and investigate problems if they happen.

Penetration Testing
When organisations employ specialists to simulate potential attacks on their network. This identifies possible weaknesses in a networks security and trying to exploit them.

Network Forensics
Investigations undertaken to find the cause of attacks on a network. This is done to prevent future attacks.

Passwords
Help prevent unauthorised users accessing the network. These should be strong and be changed regularly.

User Access Levels
Control which part of the network different groups of users can access. This helps limit the number of people with access to important data, so help prevent insider attacks on the network.

Anti-Malware Software
Designed to find and stop malware from damaging an organisations network and the devices on it. Companies use firewalls to block unauthorised access. Firewalls examine all data entering and leaving the network and block any potential threats.

Encryption
When data is translated into a code which only someone with the correct key can access, meaning unauthorised users cannot read it.

Keywords

Type of Attack	Description	Prevention
Passive	Where someone monitors data travelling on a network and intercepts any sensitive information they find. They use network monitoring hardware and software such as packet sniffers.	Data Encryption.
Active	When someone attacks a network with malware or other planned attacks.	Firewall, Anti-Virus
Denial of Service	Where a hacker tries to stop users from accessing a part of a network or website. Flooding the network with useless traffic making the network extremely slow or completely inaccessible.	Firewall
Brute Force	Type of active attack used to gain information by cracking passwords through trial and error.	Locking accounts / strong passwords.
Insider	Someone within an organisation exploits their network access to steal information.	User Access Levels.

Networks which make use of databases are vulnerable. SQL Injections are Used to access information in databases through SQL typed into a website's input box which them reveal sensitive information.

Malware is Malicious software installed on someone's device without their knowledge or consent. (e.g. scareware, spyware etc.)

Viruses attach by copying themselves to certain files. E.g. exe files. Users spread them by copying infected files and activate them by opening infected files.

Worms self replicate without any user help, meaning they can spread very quickly. They exploit weaknesses in network security.

Trojans are alware disguised as legitimate software. Users install them not realising they have a hidden purpose.