Knowledge Organiser 1.4 : Network Security

1. Forms of Attack

Malware	Software written in order to infect computers and commit crimes e.g. fraud or identify theft. Malware exploits vulnerabilities in software
Types of Malware	Malware is term that covers (among other things) viruses, trojans, worms, ransomware, spyware and adware
Phishing	Online fraud technique used by criminals. It is designed to get you to give away personal information such as usernames, passwords, bank details, credit card details… Achieved by disguising as a trustworthy source in an electronic communication, e.g. an email or fake website.
Brute Force Attack	A trial and error method used to decode encrypted data (such as passwords). Uses every combination until it hits upon the correct one.
DOS Attack	Denial of Service attack. Floods a server with useless traffic causing the server to become overloaded and unavailable
DDOS Attack	Distributed Denial of Service Attack. Using multiple computers (zombies) in a

2. Threats posed to Networks

Malware	• Files are deleted, become corrupt or are encrypted. • Computers crash, reboot spontaneously and slow down. • Internet connections become slow. • Keyboard inputs are logged and sent to hackers.
Phishing	• Accessing a victim's account to withdraw money, or purchase merchandise and services. • Open bank accounts, credit cards, cashing illegitimate cheques. • Gain access to high value corporate data. • Financial services can blacklist the company
Brute Force Attack	• Theft of data. • Access to corporate systems.
(D)DOS Attack	• Loss of access to a service for customers • Lost revenue • Lower productivity • Damage to reputation
Data Interception and Theft	• Usernames and passwords compromised • Disclosure / theft of corporate data
SQL Injection	• Contents of databases can be output, revealing private data. • Data in the database can be amended or deleted.

3. Identifying and Preventing Vulnerabilities

Malware	• Security software (Spam filter, Anti-virus, Anti-spyware, Anti-spam) • Enabling OS and security software updates. • Staff training • Backup files regularly onto removable media.
Phishing	• Strong security software. • Staff training: awareness of spotting fake emails and websites. • Staff training: not disclosing personal or corporate information. • Staff training: disabling browser pop-ups.
Data Interception and Theft	• Encryption and using virtual networks • Staff training and computer use policies
SQL Injection	• Validation on text boxes