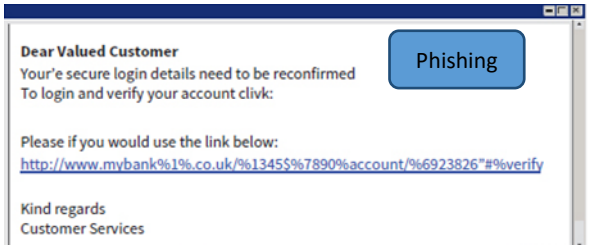
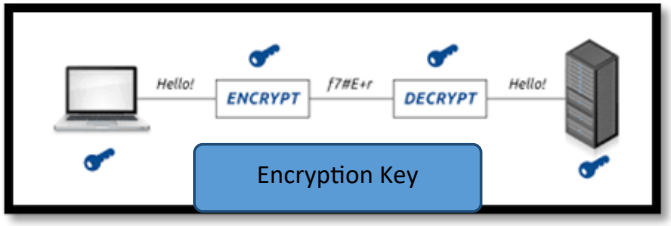
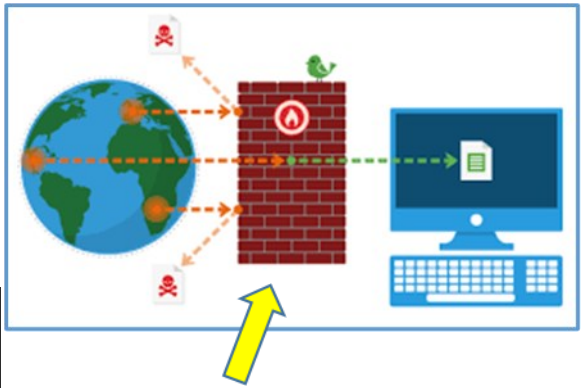
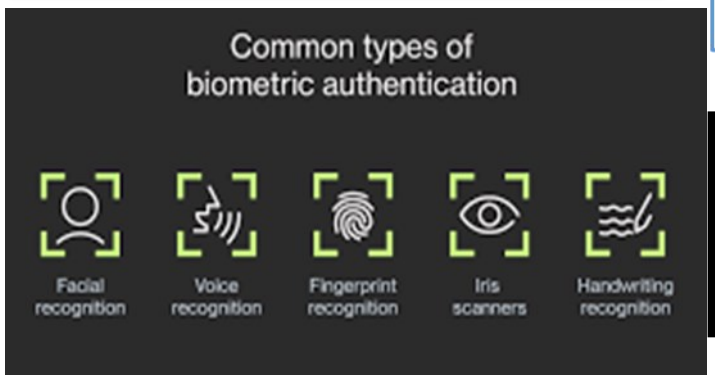
Topic 1.5 | **GCSE Computer Science** | Network Security







Firewall: A firewall is software that will block unexpected connections coming into the network. Most operating systems include a firewall.



Two-factor authentication, such as a bank ringing an accepted phone number to confirm when a new payment is set up, or a PIN and a card having to be used together.

Viruses	A *computer virus* is a **type of *computer* program** that, when executed, **replicates itself by modifying other *computer* programs and inserting its own code**
Malware	Malware (short for "**malicious software**") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behaviour an attacker wants
Worms	A computer worm is a subset of the Trojan horse malware that can **propagate or self-replicate from one computer to another without human activation** after breaching a system. Typically, a worm **spreads across a network** through your Internet or LAN (Local Area Network) connection
Trojan Horses	A type of malware that **disguises itself** as legitimate code or software.
Phishing	Phishing is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website
Social Engineering	The tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Data Interception	Data theft refers to any way sensitive information is compromised, whereas data interception is a specific type of data theft, referring to information that is captured during transmission.
Brute Force Attack	A brute force attack goes through every possible combination of a password or encryption key.
DoS	Denial of Service attack - designed to make a service inaccessible.
Botnet	Botnet refers to a network of hijacked internet-connected devices that are installed with malicious codes known as malware. Each of these infected devices is known as Bots, and a hacker/cybercriminal known as the "Bot herder" remotely controls them.
SQL Injection (Structured Query Language)	Involve adding or creating small bits of code that look like variables. However, the database server will process these as commands or programmes and do things it is not supposed to, such as destroying or modifying data or passwords in a database.
Penetration Testing	Penetration testing uses the same techniques a hacker would try, but the aim is to identify the weaknesses, rather than stealing data or damaging the system.
Anti-Malware	A type of software program created to protect information technology (IT) systems and individual computers from malicious software
Firewalls	A *Firewall* is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established
User Access Level	User access levels define what information the different users on your account can access and edit.
Passwords	A secret word or phrase that must be used to gain admission to a place.
Encryption	Uses cybersecurity to defend against brute-force and cyber-attacks, including malware and ransomware.
Cipher	Used in crypto club desert oasis
Key	An encryption key is typically a random string of bits generated specifically to scramble and unscramble data. Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable
Biometric Security	To automatically recognise people based on their behavioural or biological characteristics. The biometric technology currently used most often in physical access control is fingerprint recognition because of its lower price.

Issues