Definitions and Concepts for AQA Computer Science GCSE

Topic 6: Cyber security

Cyber Security: Consists of the processes, practices, and technologies designed to protect networks, computers, programs, and data from attack, damage, or unauthorised access.

Social Engineering Techniques: The art of manipulating people so they give up confidential information.

Malicious Code/Software (Malware): An umbrella term used to refer to a variety of forms of hostile or intrusive software.

Pharming: A cyber attack intended to redirect a website's traffic to a fake website.

Weak and Default Passwords: Passwords that are easy to guess or are pre-set by manufacturers and are not changed by the user, making systems vulnerable.

Misconfigured Access Rights: Incorrectly set permissions or privileges that allow users to access more files or systems than they need as part of their role, increasing the risk of data misuse.

Removable Media: External storage devices (e.g., USB drives, external hard drives) that can be a source of malware or data breaches if not handled securely.

Unpatched and/or Outdated Software: Software that has known security vulnerabilities because it has not been updated with the latest fixes or is no longer supported by its developer.

Penetration Testing: The process of attempting to gain access to resources without knowledge of usernames, passwords, and other normal means of access, to identify security weaknesses.

White-box Penetration Testing: A type of penetration testing where the testing team has knowledge of and possibly basic credentials for the target system, simulating an attack from inside the system (a malicious insider).

Black-box Penetration Testing: A type of penetration testing where the testing team has no knowledge of any credentials for the target system, simulating an attack from outside the system (an external attack).

Blagging (Pretexting): The act of creating and using an invented scenario (a pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.

Phishing: A technique of fraudulently obtaining private information, often using deceptive emails or SMS messages that appear to be from a legitimate source.

Shouldering (Shoulder Surfing): Observing a person's private information over their shoulder, such as cashpoint machine PIN numbers or login credentials.

Computer Virus: A type of malware that attaches itself to legitimate programs and spreads to other computers when those programs are run, often designed to damage systems or steal data.

Trojan (Trojan Horse): A type of malware that appears to be legitimate software but secretly carries out malicious functions when executed.

Spyware: A type of malware that secretly gathers information about a person or organisation without their knowledge and sends it to another entity.

Biometric Measures: Security measures that use unique biological characteristics (e.g., fingerprints, facial recognition) for authentication.

Password Systems: Security measures that rely on a secret string of characters (password) for user authentication.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart): A security measure used to differentiate between human users and automated bots, often involving distorted text or image recognition.

Using Email Confirmations: A security measure that involves sending an email to a registered address to confirm a user's identity, often for account activation or password resets.

Automatic Software Updates: A security measure where software is automatically updated to the latest version, which often includes security patches for known vulnerabilities.