Definitions and Concepts for CAIE Computer Science IGCSE

Topic 5: The internet and its uses

5.1 The internet and the world wide web

Internet: A global network of interconnected computers and devices. It provides the physical and technical infrastructure that allows data to be sent and received.

World Wide Web (WWW): A collection of websites and web pages that can be accessed via the internet using web browsers.

Uniform Resource Locator (URL): A text-based address assigned to web pages on the internet. It can contain the protocol, domain name and the web page/file name.

Domain Name: The human-readable address of a website, used instead of an IP address.

Web Page / File Name: The specific page or file on the website being requested.

Protocol: The set of rules that determines how data is transmitted between devices over a network.

HTTP (Hypertext Transfer Protocol): A protocol for transferring web pages and other content between web servers and browsers.

HTTPS (Hypertext Transfer Protocol Secure): A secure version of HTTP that encrypts communications between a web browser and a website, providing secure web transactions.

Web browser: A software application that allows users to access, retrieve, and view content on the World Wide Web.

Bookmark: A saved shortcut to a web page stored in a web browser for quick access.

User History: A record maintained by a web browser of all visited URLs along with timestamps for easy revisiting.

Tabs: Separate pages opened within a single web browser window that allow multiple web pages to be accessed simultaneously.

Cookie: A small text file stored on a user's device by a website to save information such as login details, preferences, and shopping cart contents.

Session Cookie: A temporary cookie that is deleted when the web browser is closed.

Persistent Cookie: A cookie that remains stored on the device for a set period until it expires or is deleted manually.

Domain Name Server (DNS): A server that translates a website's domain name into its corresponding IP address.

IP Address: A unique numerical address assigned to each device on a network, used to locate and communicate with web servers.

Address Bar: A section of a web browser where users can enter a URL to navigate directly to a website.

Navigation Tools: Browser buttons such as back, forward, refresh, and stop that help users control webpage loading and browsing history.

Hypertext Markup Language (HTML): The language web pages are created in. It gives control over the structure and content of pages, using tags to define elements such as text, images, and links.

5.2 Digital currency

Digital Currency: A form of money that exists only in electronic form and has no physical counterpart such as coins or notes. It can be used online to pay for goods or services.

Decentralised Digital Currency: A digital currency system that is not controlled by banks or governments.

Centralised Digital Currency: A digital currency system that is controlled by a central authority such as a bank or government.

Blockchain: A digital ledger consisting of a time-stamped series of records called blocks, which cannot be altered.

Block: A group of transactions recorded together in the blockchain, containing a block hash that links it to the previous block.

Block Hash: A unique cryptographic code that identifies a block and links it to the previous one in the blockchain.

Digital Signature: An encrypted code used to verify the authenticity of a transaction on the blockchain.

Transaction: A record of the exchange of digital currency between parties, stored in the blockchain ledger.

5.3 Cyber security

Brute-force Attack: A method where software tries many combinations of usernames and passwords to guess the correct login credentials.

Data Interception: The unauthorised capturing of data as it is sent over a network, often using special software to listen for unencrypted information such as passwords or credit card numbers.

Distributed Denial of Service (DDoS) attack: An attack that floods a website or online service with excessive traffic from multiple different senders, slowing it down or making it completely unavailable to legitimate users.

Hacking: Gaining unauthorized access to computer systems or networks by exploiting vulnerabilities or stolen credentials.

Malware (Malicious Code): A general term for harmful software designed to damage, disrupt or gain unauthorised access to computer systems.

Virus: A type of malware that attaches to legitimate files or programs and spreads when they are opened.

Worm: Malware that spreads independently through networks, by exploiting security flaws, without user action.

Trojan Horse: Malicious software disguised as a legitimate program. Once installed, it can allow hackers to access the system, steal data or install more malware.

Spyware: A type of malware that secretly collects information about a user's activities, such as keystrokes or login details, and sends it to an attacker.

Adware: Software that displays unwanted advertisements and may track user behaviour without consent. It is typically bundled with other programs.

Ransomware: Malware that encrypts files or locks users out of their systems, demanding payment for access restoration.

Phishing: Fraudulent attempts to obtain private information by pretending to be a trustworthy source, often through email or messages.

Pharming: An attack that redirects users from a legitimate website to a fake copy in an attempt to steal personal information such as login credentials or bank details.

Social Engineering: The manipulation of people into revealing confidential information by exploiting human psychology, rather than using technical hacking methods.

Access Levels: Permissions set within a system to control what data and features different users can access.

Anti-malware Software: Programs that detect, quarantine, or remove malicious software by comparing files to known malware databases.

Authentication: The process of verifying a user's identity before granting system access, using methods like passwords or biometrics.

Automated Software Updates: Automatic installation of software patches and fixes to reduce security vulnerabilities.

Firewall: A system that monitors and controls incoming and outgoing network traffic based on security rules.

Privacy Settings: Controls that allow users to manage what personal information is shared and who can access it online.

Proxy Server: An intermediary server that hides a user's IP address and filters web traffic to improve security and privacy.

Secure Socket Layer (SSL): A security protocol that encrypts data between a web browser and server to prevent interception or tampering.