ICT - ASSESSMENT

1). Define the term "cloud computing" and explain two advantages it offers to businesses.

2). Compare and contrast "fiber optic cables" and "twisted pair cables" in terms of data transmission speed and security.

3). Explain the concept of "network redundancy" and describe one method used to achieve it in computer networks.

4). Discuss the importance of "data encryption" in protecting sensitive information and outline one common encryption method.

5). Identify two potential risks associated with using public Wi-Fi networks and suggest ways to mitigate these risks.

6). Describe the process of "data backup" and explain why it is critical for organisations to regularly back up their data.

7). Explain what is meant by "Internet of Things (IoT)" and give two examples of IoT devices used in smart homes.

8). Differentiate between "static IP address" and "dynamic IP address" and provide one advantage of each.

9). Describe the role of a "firewall" in network security and outline how it helps to protect against cyber attacks.

10). Explain the term "phishing" and describe two common tactics used by phishers to deceive users.

11). Define "network latency" and discuss two factors that can contribute to high latency in a computer network.

12). Describe the difference between "server virtualisation" and "desktop virtualisation" and provide one benefit of each.

13). Explain the concept of "bandwidth" and how it affects the performance of a network.

14). Identify and describe the function of three different types of network devices.

15). Explain what is meant by "data compression" and provide an example of a lossless compression method.

16). Discuss the significance of "two-factor authentication" in enhancing account security.

17). Define "cybersecurity" and outline three best practices for maintaining good cybersecurity hygiene.

18). Explain the term "network topology" and compare the characteristics of "mesh topology" and "bus topology."

19). Describe the process of "software patching" and explain why it is important for maintaining system security.

20). Discuss the role of "DNS (Domain Name System)" in internet connectivity and describe how DNS spoofing can impact users.

21). Explain what is meant by "cloud storage" and compare it with traditional on-premises storage solutions.

22). Define "peer-to-peer (P2P) network" and give one example of how P2P networking is used in modern applications.

23). Describe the concept of "virtual private network (VPN)" and explain how it enhances privacy and security for users.

24). Identify two potential ethical concerns related to the use of artificial intelligence in ICT and discuss ways to address these concerns.

25). Explain the term "network protocol" and describe the function of TCP/IP in network communications.

ICT ASSESSMENT - Marking Scheme

(126 marks Total)

Question 1

Define the term "cloud computing" and explain two advantages it offers to businesses.

- Definition of cloud computing (2 marks)
- Explanation of two advantages (2 marks each)

Answer: Cloud computing refers to the delivery of computing services—including servers, storage, databases, networking, software, and analytics—over the internet ("the cloud").

- Advantage 1: Cost Savings (e.g., reduced IT infrastructure costs) (2 marks)
- Advantage 2: Scalability (e.g., easily scale resources up or down based on demand) (2 marks)

Question 2

Compare and contrast "fiber optic cables" and "twisted pair cables" in terms of data transmission speed and security.

- Comparison of data transmission speed (2 marks)
- Comparison of security (2 marks)

Answer:

- Fiber optic cables offer much higher data transmission speeds compared to twisted pair cables due to their ability to transmit data as light signals with minimal signal loss. (2 marks)
- Fiber optic cables provide better security as they are less susceptible to electromagnetic interference and tapping compared to twisted pair cables. (2 marks)

Question 3

Explain the concept of "network redundancy" and describe one method used to achieve it in computer networks.

- Explanation of network redundancy (2 marks)
- Description of one method (3 marks)

Answer: Network redundancy refers to the inclusion of extra or duplicate devices and paths in a network to ensure that the network remains operational even if a part of the system fails. (2 marks)

- Method: Implementing multiple network connections (e.g., dual routers or switches) to provide alternative data paths in case one connection fails. (3 marks)

Question 4

Discuss the importance of "data encryption" in protecting sensitive information and outline one common encryption method.

- Importance of data encryption (3 marks)
- Outline of one encryption method (2 marks)

Answer: Data encryption is crucial for protecting sensitive information from unauthorised access, ensuring data privacy, and maintaining data integrity during transmission or storage. (3 marks)

- Common encryption method: AES (Advanced Encryption Standard), a symmetric encryption algorithm widely used for securing data. (2 marks)

Question 5

Identify two potential risks associated with using public Wi-Fi networks and suggest ways to mitigate these risks.

- Identification of two risks (2 marks each)
- Suggestions for mitigation (1 mark each)

Answer:

- Risk 1: Man-in-the-Middle (MitM) attacks, where attackers intercept communication between the user and the network. (2 marks)
- Risk 2: Data theft, where sensitive information can be stolen by hackers on the same network. (2 marks)
- Mitigation 1: Use a VPN to encrypt internet traffic. (1 mark)
- Mitigation 2: Avoid accessing sensitive information (e.g., online banking) over public Wi-Fi. (1 mark)

Question 6

Describe the process of "data backup" and explain why it is critical for organisations to regularly back up their data.

- Description of data backup process (3 marks)
- Explanation of importance (2 marks)

Answer: Data backup involves copying and archiving data so that it can be restored in case of data loss due to hardware failure, cyber-attacks, or accidental deletion. (3 marks)

- Importance: Regular backups ensure data availability and continuity of operations in case of data loss incidents, minimising downtime and potential financial losses. (2 marks)

Question 7

Explain what is meant by "Internet of Things (IoT)" and give two examples of IoT devices used in smart homes.

- Explanation of IoT (3 marks)
- Examples of two IoT devices (1 mark each)

Answer: The Internet of Things (IoT) refers to the network of physical objects (devices) embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet. (3 marks)

- Example 1: Smart thermostat (e.g., Nest) (1 mark)
- Example 2: Smart security camera (e.g., Ring) (1 mark)

Question 8

Differentiate between "static IP address" and "dynamic IP address" and provide one advantage of each.

- Differentiation (2 marks)
- Advantage of static IP (1.5 marks)
- Advantage of dynamic IP (1.5 marks)

Answer:

- Static IP address: An IP address that remains constant and does not change over time. (1 mark)
- Dynamic IP address: An IP address that is assigned by a DHCP server and can change over time. (1 mark)
- Advantage of static IP: Consistent point of contact for remote access and hosting servers. (1.5 marks)
- Advantage of dynamic IP: Easier and more efficient IP address management in large networks. (1.5 marks)

Question 9

Describe the role of a "firewall" in network security and outline how it helps to protect against cyber attacks.

- Description of firewall role (3 marks)
- Outline of protection mechanism (2 marks)

Answer: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks. (3 marks)

- Protection: Firewalls block unauthorised access, filter out malicious traffic, and prevent cyber attacks such as malware and hacking attempts. (2 marks)

Question 10

Explain the term "phishing" and describe two common tactics used by phishers to deceive users.

- Explanation of phishing (2 marks)
- Description of two tactics (2 marks each)

Answer: Phishing is a type of cyber attack where attackers attempt to trick individuals into providing sensitive information, such as passwords or credit card numbers, by pretending to be a trustworthy entity. (2 marks)

- Tactic 1: Sending fake emails that appear to be from legitimate sources (e.g., banks, online services) to lure users into clicking malicious links. (2 marks)
- Tactic 2: Creating counterfeit websites that mimic real websites to capture login credentials and other sensitive information. (2 marks)

Question 11

Define "network latency" and discuss two factors that can contribute to high latency in a computer network.

- Definition of network latency (2 marks)
- Discussion of two factors (2 marks each)

Answer: Network latency is the delay or time taken for data to travel from the source to the destination across a network. (2 marks)

- Factor 1: Distance between devices – longer distances result in higher latency. (2 marks)
- Factor 2: Network congestion – high traffic volumes can slow down data transmission. (2 marks)

Question 12

Describe the difference between "server virtualisation" and "desktop virtualisation" and provide one benefit of each.

- Description of server virtualisation (2 marks)
- Description of desktop virtualisation (2 marks)
- Benefit of each (1 mark each)

Answer:

- Server virtualisation: The process of dividing a physical server into multiple virtual servers, each running its own operating system and applications. (2 marks)
- Desktop virtualisation: The technology that allows users to run desktop environments on virtual machines hosted on a central server. (2 marks)
- Benefit of server virtualisation: Efficient resource utilisation and cost savings by running multiple virtual servers on a single physical server. (1 mark)
- Benefit of desktop virtualisation: Centralised management and enhanced security of desktop environments. (1 mark)

Question 13

Explain the concept of "bandwidth" and how it affects the performance of a network.

- Explanation of bandwidth (2 marks)
- Impact on network performance (3 marks)

Answer: Bandwidth refers to the maximum rate at which data can be transferred over a network connection, typically measured in bits per second (bps). (2 marks)

- Impact: Higher bandwidth allows more data to be transmitted simultaneously, resulting in faster data transfer rates and improved network performance. Limited bandwidth can cause slower speeds and network congestion, affecting the overall user experience. (3 marks)

Question 14

Identify and describe the function of three different types of network devices.

- Identification of three devices (1 mark each)
- Description of each device's function (1 mark each)

Answer:

- Router: Connects multiple networks and directs data packets between them. (2 marks)
- Switch: Connects devices within a local area network (LAN) and uses MAC addresses to forward data to the correct device. (2 marks)
- Access Point: Provides wireless connectivity to devices, allowing them to connect to a wired network. (2 marks)

Question 15

Explain what is meant by "data compression" and provide an example of a lossless compression method.

- Explanation of data compression (3 marks)
- Example of lossless compression method (2 marks)

Answer: Data compression is the process of reducing the size of a data file to save storage space or speed up data transmission. (3 marks)

- Example: ZIP is a lossless compression method that reduces file size without losing any original data. (2 marks)

Question 16

Discuss the significance of "two-factor authentication" in enhancing account security.

- Significance of two-factor authentication (5 marks)

Answer: Two-factor authentication (2FA) significantly enhances account security by requiring two forms of verification before granting access: something the user knows (password) and something the user has (e.g., a mobile device). This additional layer of security makes it much harder for attackers to gain unauthorised access, even if they obtain the password. (5 marks)

Question 17

Define "cybersecurity" and outline three best practices for maintaining good cybersecurity hygiene.

- Definition of cybersecurity (2 marks)
- Three best practices (1 mark each)

Answer: Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, unauthorised access, and damage. (2 marks)

- Best Practice 1: Use strong, unique passwords for different accounts. (1 mark)
- Best Practice 2: Regularly update software and applications to patch vulnerabilities. (1 mark)
- Best Practice 3: Enable firewalls and antivirus software to detect and block threats. (1 mark)

Question 18

Explain the term "network topology" and compare the characteristics of "mesh topology" and "bus topology."

- Explanation of network topology (2 marks)
- Comparison of mesh and bus topology (3 marks)

Answer: Network topology refers to the arrangement or layout of different elements (links, nodes, etc.) in a computer network. (2 marks)

- Mesh topology: Every device is connected to every other device, providing high redundancy and reliability. (1.5 marks)
- Bus topology: All devices share a single communication line, making it simpler and cheaper to implement but prone to collisions and limited scalability. (1.5 marks)

Question 19

Describe the process of "software patching" and explain why it is important for maintaining system security.

- Description of software patching (2 marks)
- Importance for security (3 marks)

Answer: Software patching involves updating software with fixes for bugs, security vulnerabilities, and other issues identified after the software's initial release. (2 marks)

- Importance: Patching is crucial for maintaining system security as it addresses known vulnerabilities that could be exploited by attackers, thereby preventing potential breaches and maintaining system integrity. (3 marks)

Question 20

Discuss the role of "DNS (Domain Name System)" in internet connectivity and describe how DNS spoofing can impact users.

- Role of DNS (3 marks)
- Impact of DNS spoofing (2 marks)

Answer: DNS translates human-readable domain names (e.g., www.example.com) into IP addresses that computers use to identify each other on the network, enabling users to access websites and services easily. (3 marks)

- Impact of DNS spoofing: Attackers redirect users to fraudulent websites by corrupting the DNS records, leading to potential data theft, phishing attacks, and malware installation. (2 marks)

Question 21

Explain what is meant by "cloud storage" and compare it with traditional on-premises storage solutions.

- Explanation of cloud storage (2 marks)
- Comparison with on-premises storage (3 marks)

Answer: Cloud storage refers to storing data on remote servers accessed via the internet, managed by third-party providers. (2 marks)

- Comparison: Cloud storage offers scalability, remote access, and cost savings by eliminating the need for physical hardware, while on-premises storage provides greater control, security, and performance but requires significant investment in infrastructure and maintenance. (3 marks)

Question 22

Define "peer-to-peer (P2P) network" and give one example of how P2P networking is used in modern applications.

- Definition of P2P network (2 marks)
- Example of modern application (3 marks)

Answer: A peer-to-peer (P2P) network is a decentralised network where each computer (peer) acts as both a client and a server, sharing resources directly with other peers without a central server. (2 marks)

- Example: File-sharing applications like BitTorrent use P2P networking to distribute and download files among users. (3 marks)

Question 23

Describe the concept of "virtual private network (VPN)" and explain how it enhances privacy and security for users.

- Description of VPN (2 marks)
- Explanation of privacy and security enhancement (3 marks)

Answer: A virtual private network (VPN) creates a secure, encrypted connection over a less secure network, such as the internet, allowing users to access resources and transmit data as if they were directly connected to a private network. (2 marks)

- Enhancement: VPNs protect user privacy by masking IP addresses and encrypting data, making it difficult for hackers and third parties to intercept and read the information. (3 marks)

Question 24

Identify two potential ethical concerns related to the use of artificial intelligence in ICT and discuss ways to address these concerns.

- Identification of two ethical concerns (2 marks each)

- Discussion of ways to address each concern (1 mark each)

Answer:

- Concern 1: Job displacement due to automation (2 marks)
  - Addressing: Implement retraining programs to help displaced workers acquire new skills. (1 mark)
- Concern 2: Bias in AI algorithms leading to unfair treatment (2 marks)
  - Addressing: Develop and implement ethical guidelines for AI development and conduct regular audits to ensure fairness. (1 mark)

Question 25

Explain the term "network protocol" and describe the function of TCP/IP in network communications.

- Explanation of network protocol (2 marks)
- Description of TCP/IP function (3 marks)

Answer: A network protocol is a set of rules and conventions that determine how data is transmitted and received across a network. (2 marks)

- TCP/IP (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used to interconnect network devices on the internet. TCP ensures reliable data transmission by managing packet delivery, while IP handles addressing and routing of packets to their destinations. (3 marks)