CIE Computer Science

27

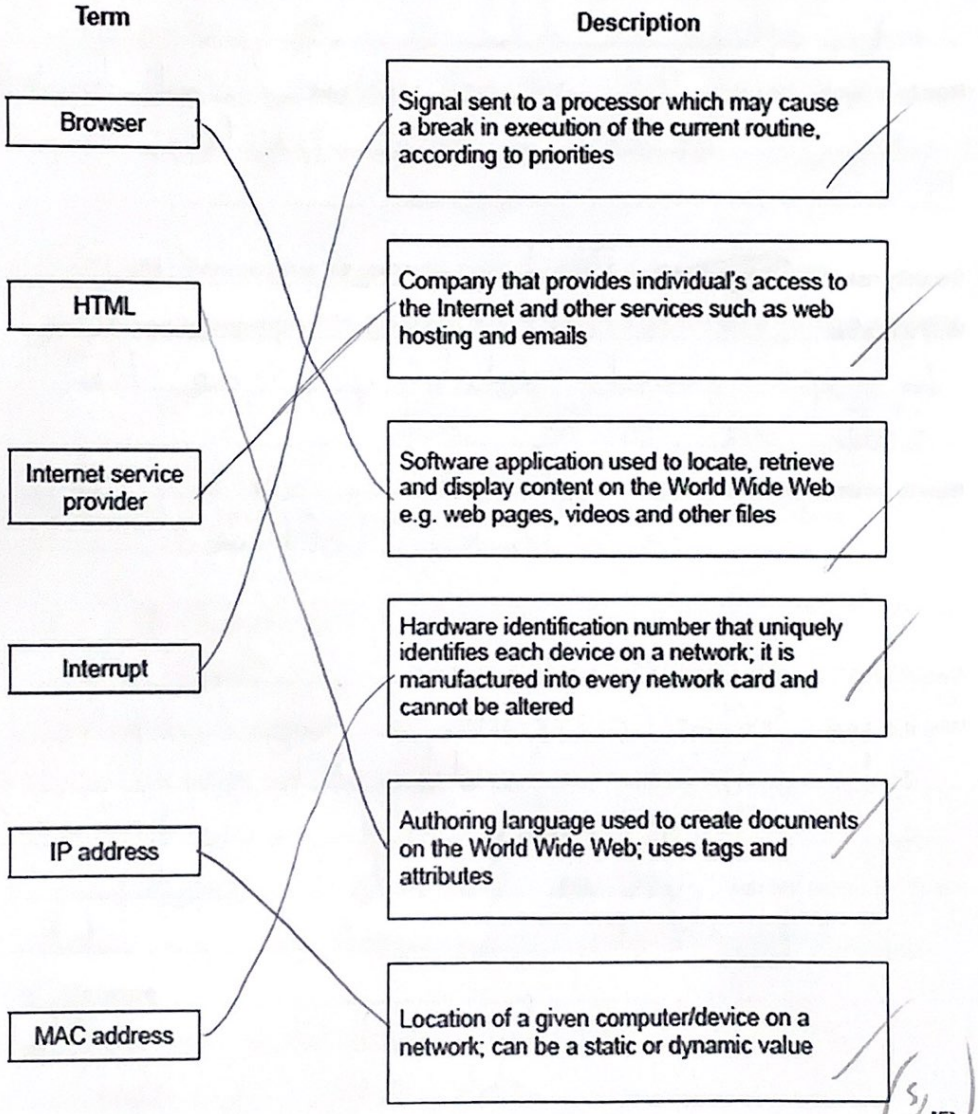
41 /41

Chapter 5 – The Internet and its uses test

Q1

Six computer terms and six descriptions are shown below.

Draw a line to link each term to its appropriate description.



5/ [5]

Q2

There are a number of security risks associated with using the Internet.

Name **three** of these risks. For each, state why it is a risk and describe how the risk can be minimised.

Security risk 1 Virus installation / malware

Why it is a risk User clicks on link and virus is installed on computer. Virus can delete files and replicate

How to minimise the risk Use antivirus software / block downloads from suspicious sites

Security risk 2 Phishing sites

Why it is a risk Link is fake, user is encouraged to input personal details which are then stolen and can be sold

How to minimise the risk Do not click on suspicious links / use a blocking software

Security risk 3 DDoS attacks

Why it is a risk Software is installed on many computers and a botnet is created which sends many simultaneous requests to the targeted server, flooding it / bringing it down / crashing it

How to minimise the risk Use a firewall to block unwanted attacks

9

[9]

Q3

David has installed anti-virus software on his computer.

(a) State **three** tasks carried out by anti-virus software.

Task 1 Regular and automatic scans of all files on computer

Task 2 Deletion / wiping of files containing malicious code (which may be virus)

Task 3 Automatic virus definitions updates to ensure latest viruses are taken into account (3)

[3]

(b) David is still concerned that his computer might get infected by a computer virus.

State **three** other ways in which David can reduce the risk of his computer getting a computer virus.

1 Use firewall on computer

2 Do not click on suspicious links

3 Use automatic site blocker / link verification to block suspicious / malicious websites (3)

[3]

4) Use biometric password

Q4) Explain each of the following terms:

a) **Hacker**

A perpetrator who steals a file victim's data by injecting malicious code into their device (2)

[2]

b) **Malware**

Malicious code that harms the device or steals the user's data (2)

[2]

c) **Virus**

Malicious software that propagates and replicates itself, having user's device and also perhaps removing files (2)

[2]

d) **Spyware**

Software which records users key presses / actions to find out their personal details / password (2) and use these for unsavoury purposes

[2]

5). Explain the difference between a dynamic IP address and a static IP address

• Dynamic IP address can change and is reassigned every time the user connects to a different network. (within network only), making it not always identifiable IPv6

• Static IP address cannot be changed (is set by manufacturer) and remains assigned to a specific entity, making it identifiable IPv4

• These help to combat the problem of not enough IP addresses [3]

3/3

6)

A company has a website that is stored on a web server.

(a) The website data is broken down into packets to be transmitted to a user.

Describe the structure of a data packet.

• Packet header
  • contains originator's IP address, destination IP address and packet number
• Payload - contains data to be transmitted
• Trailer - marks end of packet

[4]

4

(b) The website hosts videos that users can stream. The company uploads new videos to the website.

(i) The videos are compressed before they are uploaded to the website.

Tick (✓) **one** box to show which statement is a benefit of compressing the videos.

A	Data is encrypted.	☐
B	Duration of each video will be reduced.	☐
C	Less storage space on the web server is required.	✓
D	More bandwidth is required when viewing the videos.	☐

1/1

[1]

The company is concerned about a distributed denial of service (DDoS) attack.

(i) Describe what is meant by a DDoS attack.

- Many innocent users computers have malware / virus installed on computers via a suspicious link
- Perpetrator uses this to create a botnet
- When the perpetrator wants, the botnet simultaneously starts sending many requests to one target web server, which as a result crashes and is temporarily or permanently not working, causing website owner to not work [4]

4/4

(ii) Suggest **one** security device that can be used to help prevent a DDoS attack.

Firewall [1]

1