CHAPTER 5 – FULL CHAPTER WORKSHEET ANSWERS

5.1 The internet and the world wide web

MJ2019 / 12

(d)	**One** from: – Uniform resource locator – The website's address – User friendly version of the IP address

MJ2019/13

stion	Answer
(d)	1 mark for each correct term, in the correct place: – URL – https – Domain name – Web server – Browser – HTML

MJ2019/12

6(b) 1 mark per each correct row.

Statement	True (✓)	False (✓)
Cookies can be used to store a customer's credit card details	✓	
Cookies can be used to track the items a customer has viewed on a website	✓	
Cookies will corrupt the data on a customer's computer		✓
Cookies are downloaded onto a customer's computer	✓	
Cookies can be deleted from a customer's computer	✓	

MJ2019/13

(e)(i)	– Small packets of data – … that are stored by the web browser
(e)(ii)	**Four** from: – To store a customer's password … – To store a customer's credit card details … – … so they do not need to be re-entered in future – To track what the customer has viewed on the website … – … so she can send them adverts that match their preferences

ON2019/11

(b)(i)	**One** from: ∞ Protocol is HTTPS ∞ Padlock icon is locked ∞ Can view website certificate

ON2019/12

(b)	**Three** from: ∞ Display a web page ∞ Sends a request to the web server ∞ Receives data from web server ∞ Translates HTML files ∞ Processes client-side script, e.g. JavaScript ∞ Store favourites ∞ Store history ∞ Navigation forward and backward ∞ Check security ∞ Store / access cookies ∞ Find specific text within a web page ∞ Downloading file from the web ∞ Allows a homepage ∞ Allows multiple tabs / web pages to be opened ∞ Stores data in its cache
(c)	**Three** from: ∞ Hypertext Transfer Protocol Secure // It is a protocol … ∞ … that is a set of rules/standards ∞ Secure version of HTTP ∞ Secure website // secures data ∞ Uses TLS / SSL ∞ Uses encryption

MJ2020/13

(ii)	Any **four** from: – requests web server to identify itself/view the (SSL) certificate – receives a copy of the (SSL) certificate, sent from the webserver – checks if (SSL) certificate is authentic/trustworthy – sends signal back to webserver that the certificate is authentic/trustworthy – starts to transmit data once connection is established as secure

MJ2021/12

6(a)	Any **three** from: – Webserver sends (cookie) file to user's **browser** – User's payment details stored in **encrypted** text file // data is encrypted to be stored – Cookie file is stored by **browser/on user's HDD/SSD** – When user revisits website, **webserver** requests cookie file // **webserver** can access the data stored in the cookie file (to automatically enter details) – … and **browser** sends cookie file back to **webserver** (to automatically enter the details)

6(b)	**Four** from: – User does not see what information is stored // might collect data that user does not know about … – … so, user may feel their privacy is affected – A profile could be built about the user … – … that could expose a user's identity // lead to identity theft – Sensitive information stored in cookies could be intercepted in transmission … – Other websites could gain access to the cookies stored on a user's computer … – Computer could be hacked to obtain data stored in cookies … – … so, payment information could be stolen and used by a third party

ON2021/11

11 One mark per each correct term.

Terms	Description
HTML	the language used to create a web page
Browser	the type of software application used to display a web page
IP address	an address given to a computer, by a network, to allow the computer to be uniquely identified
Cookie	a text file sent by a web server to collect data about a user's browsing habits
Internet Service Provider // ISP	the company that provides a connection to the Internet

MJ2022/13

uestion	Answer
4(a)	**Three** from: • Protocol • Domain name / Web server name • Filename / web page name / folder name

uestion	Answer
4(b)	• It is sent to a DNS … • which looks up the **corresponding/matching IP** address

MJ2023

(e) Any **four** from:

- Session cookies are stored in memory/RAM
- … whereas persistent cookies are stored on the hard drive/secondary storage
- When the browser is closed a session cookie is lost
- … whereas a persistent cookie is not lost
- … until deleted by the user/they expire

ON2023/12

9

Term	Description
world wide web	the collective name for all the web pages available
cookie	a small text file, stored by the web browser, that can store a user's personal data
uniform resource locator (URL)	the **text-based address** for a website // It is made up of the protocol, domain name and filename/folder name
web server	Stores **web pages** // receives requests from clients and returns requested web page
hypertext markup language // HTML	the language used to create a website. Example tags are <head> and <body>
hypertext transfer protocol // HTTP	a protocol that is used to request and send web pages

ON2023/13

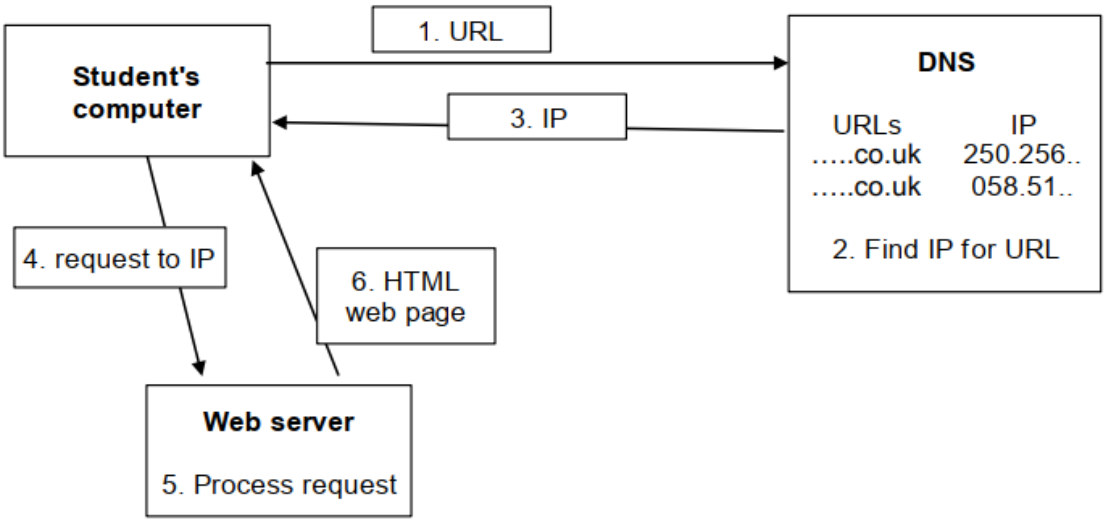
Question	Answer	Marks
4(a)	Any **two** from: – Display web pages – … by rendering HTML	**2**
4(b)	– Storing cookies	**1**
4(c)	Any **one** from: – Storing bookmarks – Storing favourites	**1**

FM2024/12

4

Any **five** marks for each part of diagram:

- **URL** from computer/browser to DNS
- DNS storing table/database of **URL** and **IPs** // DNS finding **IP** for **URL**
- DNS sending **IP** to computer / browser
- DNS sending to higher DNS if not found
- Web browser/computer sending request to **IP** of **web server**
- **Web server** processing request
- Web page data sent from **server** to computer / web browser



MJ2024/12

11(a)

Any **two** from:

- The internet is the infrastructure
- The world wide web is a collection of web pages

MJ2024/13

(e)

Any **six** from:

- The users type the **URL** into the **address bar/web browser**
- The web browser sends the **URL** to the **DNS**
- The **DNS** searches for the **matching IP address**
- The **DNS** returns the **IP address** to the web browser
- If the DNS cannot find the IP address it sends the URL to the next DNS
- The web browser sends a **request to the IP address/web server**
- The **web server** sends the data for the web page to the web browser
- The web browser **renders the HTML** data to display the web page

ON2024/13

4

One mark for each correct term or description in the correct place.

Term

- World wide web // WWW
- IP (address)
- Domain name server // DNS

6(a)	**One** mark for each correct term in the correct order: • web browser • session • temporary • web browser // session • persistent • permanent • expire
6(b)	Any **three** from: For example: • User preferences // by example • Login details • Payment details • User's **personal** details e.g. address • Contents of a shopping cart • Targeted advertising

FM2025/12

(c)(i)	1 mark from ● The collection of websites and web pages accessed using the internet ● The websites hosted on the internet/web servers
(c)(ii)	1 mark each to max 4 ● Uses SSL/TSL ● Encrypts data ● … using asymmetric encryption ● … data is encrypted using the web server's public key ● … data can only be decrypted by the web server's private key ● Data transmitted to the server can only be decrypted by the server

5.2 Digital currency

ON2023/12

12(a)	Any **two** from: – Only exists electronically – Can be a decentralised system – Can be a centralised system – Usually encrypted
12(b)	– Blockchain

FM2024/12

5

One mark for each term in correct place:

- physically
- blockchains
- time-stamp
- traced

A digital currency does not exist **physically**, it can only be accessed electronically.

Some digital currencies have digital ledgers called a **blockchains**. These are decentralised databases where each transaction is stored as a new set of data with a **time-stamp** and is linked to the previous set of data. This means that transactions cannot be altered, only new transactions added, which allows the location of the data to be **traced**.

ON2024/11

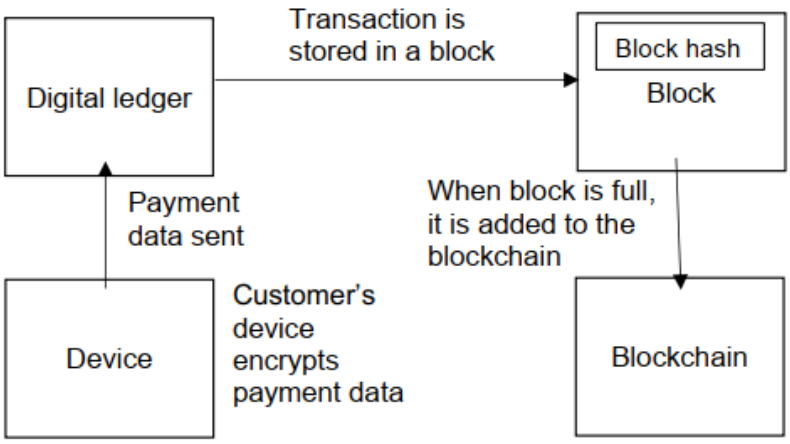
8

One mark for each correct part.

The diagram shows:

- Digital **ledger** is used
- Device encrypting data
- Device sending data to digital **ledger**
- Payment being recorded on digital **ledger**
- … including details such as digital signature/time/date stamp
- Transaction is stored in a block …
- … in multiples
- Each block has block hash/unique identifier
- When block is executed or full
- … it is applied to every device that has the blockchain // Block is added to blockchain (on each device)

For example:



MJ2025/11

(c)(i)	A currency that only exists electronically/virtually
(c)(ii)	Blockchain

MJ2019/11

4(a)(i)	1 mark for security method, 2 marks for description **Anti-virus (software) // Anti-malware (software)** • Scans the computer system (for viruses) • Has a record of known viruses • Removes/quarantines any viruses that are found • Checks data before it is downloaded • … and stops download if virus found/warns user may contain virus **Firewall // Proxy server** • Monitors traffic coming **into and out of** the computer system • **Checks** that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist
4(a)(ii)	1 mark for security method, 2 marks for description **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i)** **Passwords** • Making a password stronger // by example • Changing it regularly • Lock out after set number of attempts // stops brute force attacks // makes it more difficult to guess **Biometrics** • Data needed to enter is unique to individual • … therefore very difficult to replicate • Lock out after set number of attempts **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • … making it more difficult for hacker to obtain it • Data has to be entered into the same system • … so if attempted from a remote location, it will not be accepted
4(a)(iii)	1 mark for security method, 2 marks for description **Anti-spyware software // Anti-malware (software)** • Scans the computer for spyware • Removes/quarantines any spyware that is found • Can prevent spyware being downloaded **NOTE: Anti-malware (software) cannot be awarded if already given in 4(a)(i)** **Drop-down boxes // onscreen/virtual keyboard** • Means key logger cannot collect data // key presses cannot be recorded • … and relay it to third party **Two-step verification // Two-factor authentication** • Extra data is sent to device, pre-set by user • … making it more difficult for hacker to obtain it • Data has to be entered into the same system • … so if attempted from a remote location, it will not be accepted **NOTE: Cannot be awarded if already given in 4(a)(ii)** **Firewall // proxy server** • Monitors traffic coming into and out of the computer system • Check that the traffic meets any criteria/rules set • Blocks any traffic that does not meet the criteria/rules set // set blacklist/whitelist **NOTE: Cannot be awarded if already given in 4(a)(i) or 4(a)(ii)**

6(a) **Four** from (max 2 marks per improvement):

- Make the password require more characters
- Makes the password harder to crack/guess
- More possible combinations for the password

- Make the password require different types of characters
- Makes the password harder to crack/guess
- More possible combinations for the password

- Use a biometric device
- Hard to fake a person's biological data // data is **unique**

- Two-step verification // Two factor-authentication
- Adds an additional level to hack
- Have to have the set device for the code to receive it
- Drop-down boxes // onscreen keyboard
- To prevent passwords being obtained using keylogger

- Request random characters
- Won't reveal entire password

- Set number of password attempts
- Will lock account if attempting to guess
- Will stop brute-force attacks

8(a) **Six** from:

- SSL is a (security) protocol
- It encrypts any data that is sent
- It uses/sends digital certificates …
- … which is sent to the (buyer's/user's) browser // requested by (buyer's/user's) browser
- … that contains the gallery's public key
- … that can be used to authenticate the gallery
- Once the certificate is authenticated, the transaction will begin

(b) 1 mark for each correct tick.

Statement	True (✓)	False (✓)
Firewalls are only available as hardware devices		✓
Firewalls allow a user to set rules for network traffic	✓	
Firewalls will automatically stop all malicious traffic		✓
Firewalls only examine traffic entering a network		✓
Firewalls encrypt all data that is transmitted around a network		✓
Firewalls can be used to block access to certain websites	✓	

MJ2019/12

5

- Password protection
- **Password** is released on the **release date**

- Encryption
- Encryption **key** is released on the **release date**

MJ2019/13

3(a)	**Four** from: – The company could use the firewall to set criteria – Gaming websites can be listed as blocked websites // ports can be blocked – The firewall would examine any traffic leaving the network – If it detected traffic requesting a listed website, it will block access to it – Keeps a log of all attempts to access blocked websites

3(c)	**Six** from: – The user could have been sent an email with an attachment / link containing the spyware – The user could have clicked a link on an untrusted website – When the attachment / link was clicked the spyware was downloaded onto the user's computer – The spyware recorded all the key logs from the user's keyboard – The recorded key logs were sent back to the creator of the spyware – The key logs were analysed – A common pattern / word in the key logs could have allowed a password to be identified

MJ2019/13

(b)	**One** mark for identified method, **one** mark for how it prevents spyware: **Two-step verification // Two-factor authentication** ∞ Extra data is sent to device making it more difficult for hacker to obtain it ∞ Data has to be entered into the same system // if attempted from a remote location, it will not be accepted **Use a biometric device** ∞ The person's biological data (e.g. their fingerprint) is also required

ON2019/13

8	**Four** from: ∞ A hacker could have hacked the network … ∞ … and downloaded the malware onto the network ∞ Clicking a link/attachment/downloaded a file from an email/on a webpage … ∞ … the malware could have been embedded into the link/attachment/file ∞ Opening an infected software package … ∞ … this would trigger the malware to download onto the network ∞ Inserting an infected portable storage device … ∞ … when the drive is accessed the malware is downloaded to the network ∞ Firewall has been turned off … ∞ … so malware would not be detected/checked for when entering network ∞ Anti-malware has been turned off … ∞ … so malware is not detected/checked for when files are downloaded

MJ2020/12

10(a)	**One** mark for similarity, **two** marks for differences Similarity: – Both are designed to steal personal data – They both pose as a real company/person Differences: – Pharming uses malicious code installed on hard drive – Phishing is in form of an email – Phishing requires use to follow a link / open an attachment
10(b)	– Virus – Malware
10(c)(i)	– Incorrect

ON2020/12

(ii)	Any **four** from: – Acts as a firewall – Monitor/filters/examines incoming **and** outgoing traffic – Rules/criteria for traffic can be **set** // blacklist/whitelist **set** – Blocks any traffic that does not meet criteria … – … and can send a warning message **to the user** – Stop the website failing in a DoS attack // DoS attack hits the proxy server and not the webserver

MJ2022/11

7(a)	Any **one** from: • Uses biological data • It uses **characteristics/features** that belong to a **human**
7(b)	Any **two** from: • A biometric password cannot be guessed • It is very difficult to fake a biometric password • A biometric password cannot be recorded by a keylogger/spyware • A perpetrator cannot shoulder surf to see a biometric password

MJ2022/12

6(a)	**One** mark for identifying the attack, **two** marks for the description • Phishing • Email is sent to user to encourage them to click link • … that takes user to fake website Pharming • Email is sent to user to encourage them to click link/download attachment • … that triggers **download** of **malicious code** that will redirect user to fake website Virus/malware • Email is sent to user to encourage them to click link/download attachment • … that triggers **download** of virus/malware Denial of service // DoS • A very large number of emails are sent to a **server/network at the same time** • … crashing the **server/network**

(b)

One mark for identification. E.g. **One** mark per bullet for description to **max two** each.

Virus
- Software/code that replicates
- …when the user runs it // with an active host
- Deletes/damages/corrupts data/files // takes up storage/memory space

Worm
- Software/code that replicates itself on a **network**
- …without user input // without active host
- Takes-up bandwidth
- Deletes/damages/corrupts data/files // takes up storage/memory space
- Opens back doors to computers over the network
- Used to deposit other malware on networked computers

Trojan horse
- Software/code that is hidden within other software // Software that is disguised as authentic software
- …when **downloaded/installed** the other **malware/by example** it contains is **installed**

Adware
- Software/code that generates/displays (unwanted) adverts on a user's computer
- Some may contain spyware/other malware
- Some when clicked may link to viruses
- Reduces device performance // reduces internet speed
- Redirects internet searches/user to fake websites

Ransomware
- Software/code that stops a user accessing/using their computer/data
- …by encrypting the data/files/computer
- A **fee** has to be paid to decrypt the data // A **fee** has to be paid to 'release' the computer/device/data

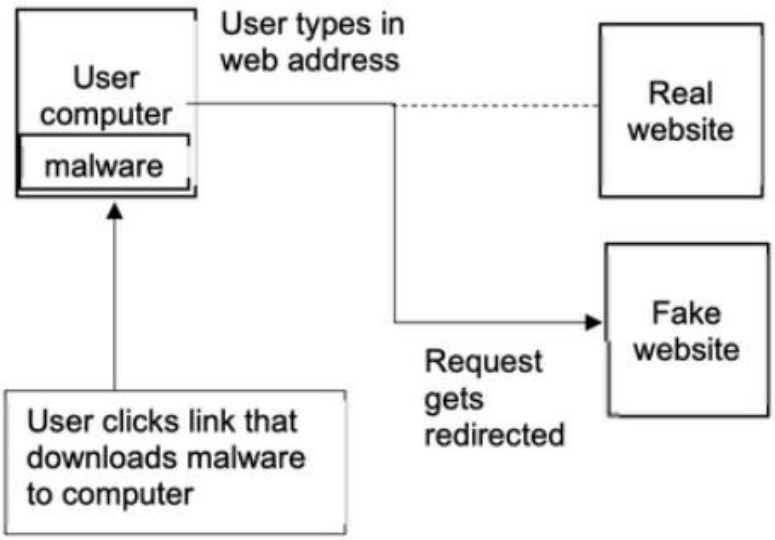
(c)

One mark for each similarity to **max two**. **One** mark for difference (both sides needed unless clearly and accurately implied).

Similarities e.g.
- Check incoming and outgoing signals // filter traffic
- Store whitelist/blacklist
- Block incoming/outgoing signals
- Both block unauthorised access
- Keep a log of traffic
- Both can be hardware or software (or both)

Differences e.g.
- Proxy can hide user's IP address, firewall does not hide the user's IP address
- Proxy intention is to divert attack from server, firewall is to stop unauthorised access
- Proxy protects a server, firewall protects individual computer
- Proxy examines/processes requests for a website but a firewall does not (checks type of signal) // Proxy **processes** client-side requests whereas firewall **filters** packets
- Proxy transmits website data to the user, but a firewall does not (it allows valid signals)
- Proxy allows faster access to a web page using cache, but a firewall does not (allow faster access or have cache)
- Proxy can hide internal network from internet, but a firewall cannot

MJ2023/11

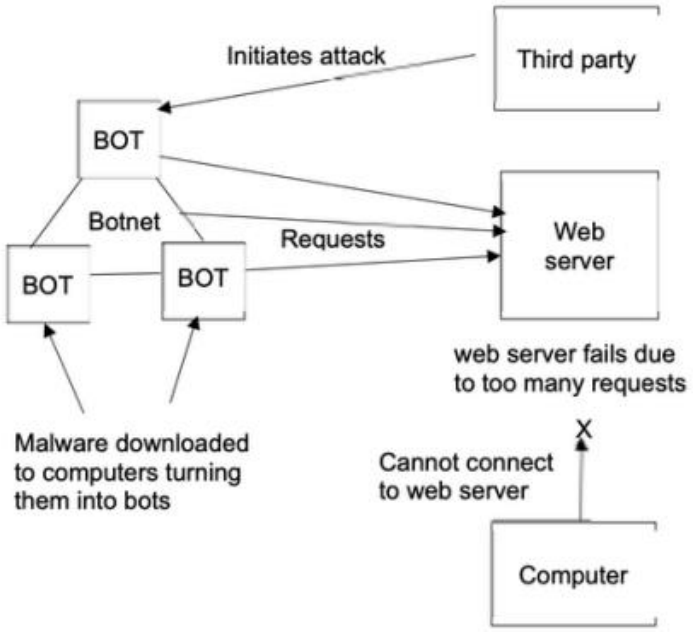
8(a)	**Three** from: • Trial and error to **guess** a **password** • **Combinations** are repeatedly entered … • … until correct password is found • Can be carried out manually or automatically by software
8(b)(i)	Any **two** from: e.g. • Steal/view/access data • Delete data • Change data • Lock account // Encrypt data • Damage reputation of a business
(c)	Any **two** from: • Two-step verification//Two-factor authentication//by example • Biometrics • Firewall // Proxy-server • **Strong/complex** password // by example • Setting a limit for login attempts • Drop-down boxes • Request for partial entry of password
(b)	**One** mark for each correct part of the diagram. Diagram shows: • User clicks/opens attachment/link that triggers download • Malicious software downloaded onto user's computer • User enters website address • User is **redirected** to fake website e.g. 

MJ2023/12

7(a)

One mark for each part of the diagram (MAX six).
The diagram demonstrates:

- Malware downloaded to several computers
- … turning it into a bot/zombie
- … creating a network of bots/zombies
- Third party/hacker initiating the attack
- **Bots** send requests to a web **server** at the same time
- The web **server** fails due to the requests
- Legitimate requests cannot reach the web server



MJ2023/13

(b)

Two marks for description, **one** mark for example:

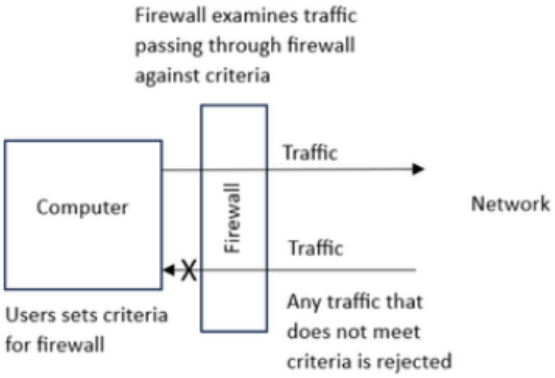
- Manipulating / deceiving / tricking people …
- … to obtain data // to force them to make an error
- Any suitable example of social engineering

(c)

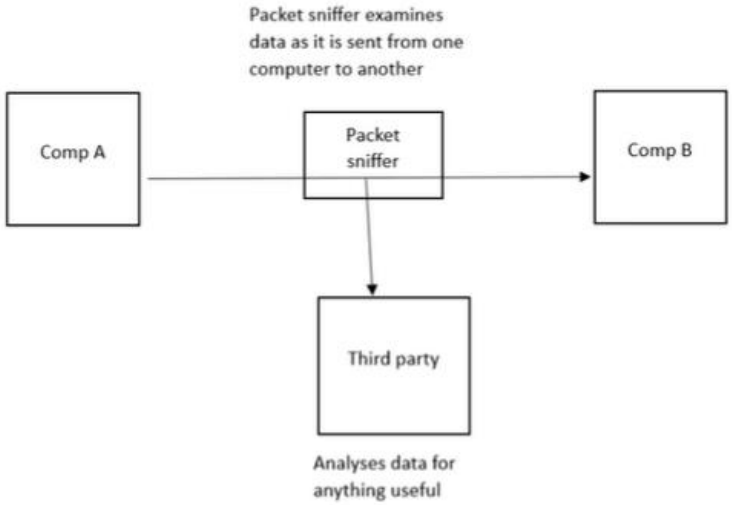
Any **three** from:

- Providing users with different **permission** for the data
- Limiting access to reading data limiting the data that can be viewed
- Limiting access to editing data // limiting the data that can be deleted / changed
- Normally linked to a username

ON2023/11

6	The diagram includes (any **four** from): – Traffic passing both ways through the firewall – An indication that criteria is set for the firewall – Traffic is compared to criteria – Traffic being rejected if it does/does not meet criteria – Traffic being accepted if it does/does not meet criteria e.g. 

ON2023/12

8(a)	The diagram demonstrates (**One** mark for each part of the diagram): – Data is being sent from one device to another – The data is being examined **during transmission** – Packet sniffer is used – Intercepted data is reported to a third-party **during transmission** … – … and analysed for anything useful – Connection hacked to spoof destination address e.g. 
8(b)	– Encryption … – … if the data is intercepted it will be **meaningless** (because they do not have the decryption key)

ON2023/13

(d)	Any **one** from: – It encrypts it – Uses digital certificates	**1**

MJ2024/13

(d)(i)	Any **three** from: • DDoS // DoS • Hacking • Malware // by example • Brute-force attack NOTE: three different examples of malware can be awarded.
(d)(ii)	Any **two** from: • Can **limit** the **number of requests** sent to the web server at a time • Can process **common requests** that will not need to enter the network • Act as a firewall • Examine incoming data to the webserver/network • Can have set rules/criteria for data to meet • Can have a blacklist/whitelist/list of IP addresses to block • **Blocks** traffic that **doesn't meet criteria** • Closing certain ports

MJ2025/12

(ii)	Any **six** from: • Encrypted connection established … • … using asymmetric encryption • … to make any data sent meaningless • The **web browser** asks the **web server** to identify itself. • … by sending its digital certificate. • The digital certificate is authenticated/validated by the **web browser**. • If the certificate is authenticated/valid, the connection is secure/the transaction can begin. • If the certificate is not authenticated/invalid, the connection is not secure/the transaction is cancelled/rejected/user is notified