5. The Internet and Its Uses

5.3 Cyber security

Marking scheme

Q1)

1 mark per correct word

1 protocol

2 web server name

3 file name

accept these three items in any order

HTML tags/text

firewall

proxy server

[6]

Q2)

(a) virus

any **two** from:

- program/software that replicates/copies itself
- can delete or alter files/data stored on a computer
- can make the computer "crash"/run slow

pharming

any **two** from:

- malicious code/software installed on a user's hard drive/actual web server
- this code redirects user to a fake website (without their knowledge)
- to obtain personal/financial information/data

phishing

any **two** from:

- legitimate-looking emails sent to a user
- as soon as recipient opens/clicks on link in the email/attachment …
- … the user is directed to a fake website (without their knowledge)
- To obtain personal/financial information/data

[6]

(b) (i) Any **two** from:

- spyware/key logging software can only pick up key presses
- using mouse/touchscreen means no key presses to log
- the numbers on the key pad are in random/non-standard format, which makes it more difficult to interpret

[2]

(ii) **1** mark for name and **1** mark for description

any **one** from:

chip and PIN reader
– only the user and the bank know which codes can be generated

request user name
– additional security together with password/PIN

anti-virus
– removes/warns of a potential virus threat which can't be passed on to customers

firewall
– (helps) to protect bank computers from virus threats and hacking

encryption
– protects customer data by making any hacked information unreadable

security protocol
– governs the secure transmission of data

Biometric
– to recognise user through the use of, e.g. facial/retina/finger print

Alerts
– users IP/MAC address is registered and user is alerted through, e.g. SMS if account is accessed through an unregistered address

[2]

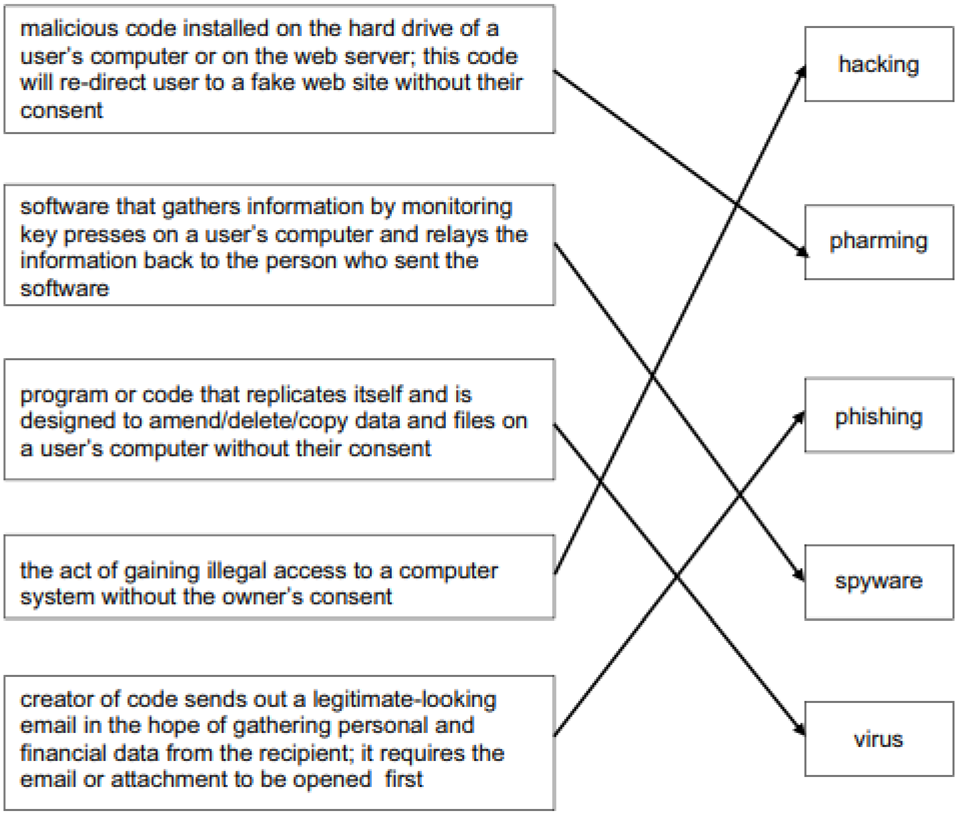
Q3)

(a) 1 mark per correctly placed tick

Statement	True	False
they are a form of spyware		✓
they are used in advertising only		✓
they are used to track the browsing of a user	✓	
they act in the same way as a virus		✓

[4]

(b)



malicious code installed on the hard drive of a user's computer or on the web server; this code will re-direct user to a fake web site without their consent

software that gathers information by monitoring key presses on a user's computer and relays the information back to the person who sent the software

program or code that replicates itself and is designed to amend/delete/copy data and files on a user's computer without their consent

the act of gaining illegal access to a computer system without the owner's consent

creator of code sends out a legitimate-looking email in the hope of gathering personal and financial data from the recipient; it requires the email or attachment to be opened first

hacking

pharming

phishing

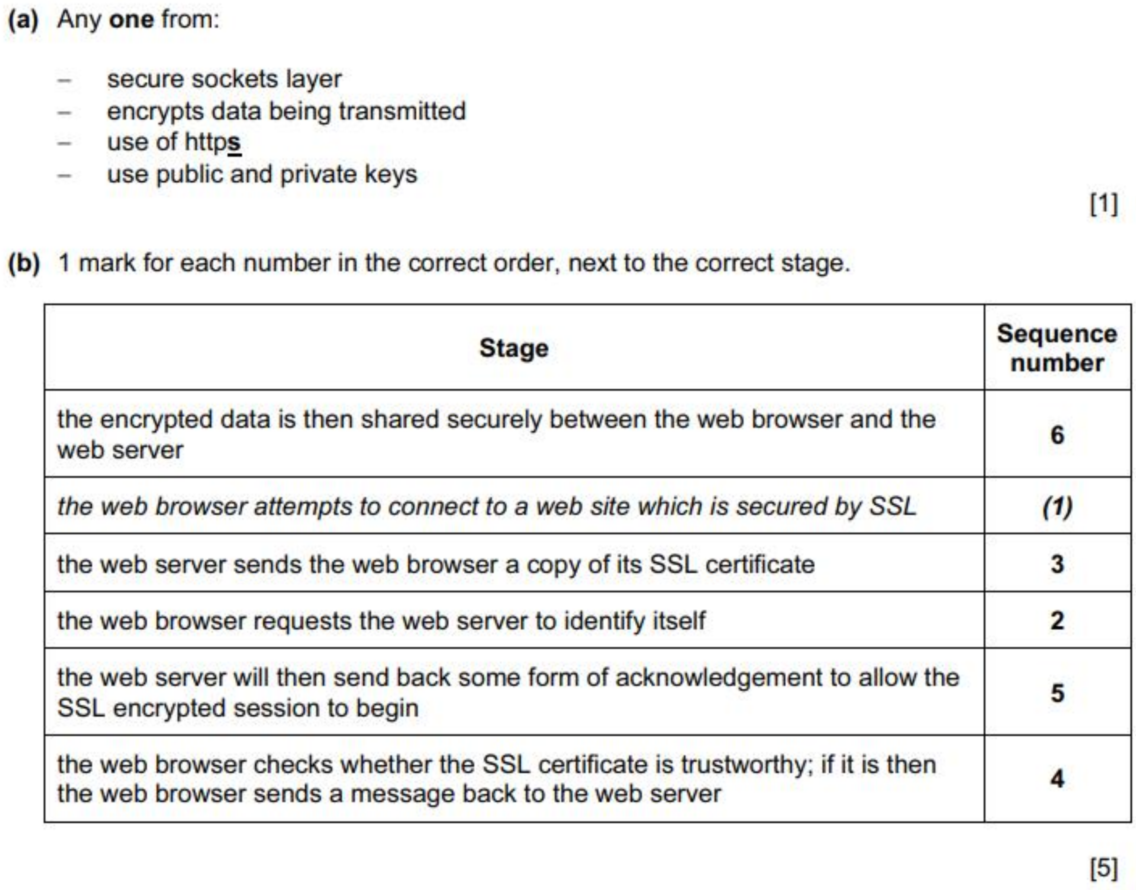
spyware

virus

4/5 matches – 4 marks
3 matches – 3 marks
2 matches – 2 marks
1 match – 1 mark

[4]

Q4)



(a) Any **one** from:

- secure sockets layer
- encrypts data being transmitted
- use of http**s**
- use public and private keys

[1]

(b) 1 mark for each number in the correct order, next to the correct stage.

Stage	**Sequence number**
the encrypted data is then shared securely between the web browser and the web server	**6**
the web browser attempts to connect to a web site which is secured by SSL	***(1)***
the web server sends the web browser a copy of its SSL certificate	**3**
the web browser requests the web server to identify itself	**2**
the web server will then send back some form of acknowledgement to allow the SSL encrypted session to begin	**5**
the web browser checks whether the SSL certificate is trustworthy; if it is then the web browser sends a message back to the web server	**4**

[5]

Q5)

1 mark per correct word

Freeware

Shareware

Free software

(Computer) Ethics

Plagiarism

[5]

Q6)

(a) Firewall [1]

(b) Shareware [1]

(c) SSL (secure socket layer) (accept HTTPS and TLS) [1]

(d) MIDI [1]

(e) Microphone [1]

Q7)

1 mark for each risk + 1 mark for corresponding reason why it is a risk and 1 mark for method of minimisation

Risk:	hacking
Reason:	illegal/unauthorised access to data deletion/amendment of data
Minimised:	use of passwords/user ids use of firewalls encrypt data/encryption

Risk:	virus
Reason:	can corrupt/delete data cause computer to crash/run slow can fill up hard drive with data
Minimised:	use of /run anti-virus (software) do not download software or data from unknown sources

Risk:	spyware/key logging (software)
Reason:	can read key presses/files/monitors on a user's computer
Minimised:	use of/run anti-spyware (software) use data entry methods such as drop-down boxes to minimise risk

Risk:	phishing
Reason:	link/attachments takes user to fake/bogus website website obtains personal/financial data
Minimised:	do not open/click emails/attachments from unknown sources some firewalls can detect fake/bogus websites

Risk:	pharming
Reason:	redirects user to fake/bogus website redirection obtains personal/financial data
Minimised:	only trust secure websites, e.g. look for http**s** check the URL matches the intended site

Risk:	credit card fraud/identity theft
Reason:	loss of money due to misuse of card/stealing data
Minimised:	set passwords encrypt data/encryption

Risk:	cracking
Reason:	illegal/unauthorised access to data
Minimised:	setting strong passwords encrypt data/encryption

There may be other valid answers given that are outside the provided mark scheme.

[9]

Q8)

(a) **(i)** Free software / open source software [1]

(ii) Any **three** from:
– Set of principles / laws that regulate the use of computers
– Covers intellectual property rights (e.g. copying of software)
– Privacy issues (e.g. accessing personal information)
– Impact of computers on society (relevant examples can be credited) [3]

(b) 1 mark for each CORRECT row

Statement	**Firewall**	**Proxy server**
Speeds up access of information from a web server by using a cache		✓
Filters all Internet traffic coming into and out from a user's computer, intranet or private network	✓	✓
Helps to prevent malware, including viruses, from entering a user's computer	✓	
Keeps a list of undesirable websites and IP addresses	✓	✓

[4]

(c) **one** mark for method + **one** mark for linked reason (maximum 6 marks)

– back up files…
– …on a regular basis / to another device / to the cloud

– set data to read only…
– …to prevent accidental editing

– save data on a regular basis…
– …to prevent loss / corruption of data in unexpected shutdown / failure

– use correct shut down / start up procedures…
– …to prevent damage to components / stored files

– use correct procedures before disconnecting portable storage device…
– …to prevent damage to device / data corruption

– keep storage devices in a safe place…
– …away from fire hazards [6]

Q9)

Any **two** from:
– facial recognition software / biometric software used to scan face
– face image converted to digital format / data by the camera
– digital image formed from scanned photo / biometric data stored in passport
– key features of the face are checked / compared [2]

Q10)

1 mark for each correct column

Software feature	**Free**	**Freeware**	**Shareware**
Software source code can be freely accessed and modified as required	✓		
All the features of the full version of the software are not made available; the full version needs to be purchased first			✓
The original software is subject to all of the copyright laws		✓	✓
It is possible to distribute modified versions or copies of the software to friends and family	✓		
	(1 mark)	(1 mark)	(1 mark)

[3]

Q11)

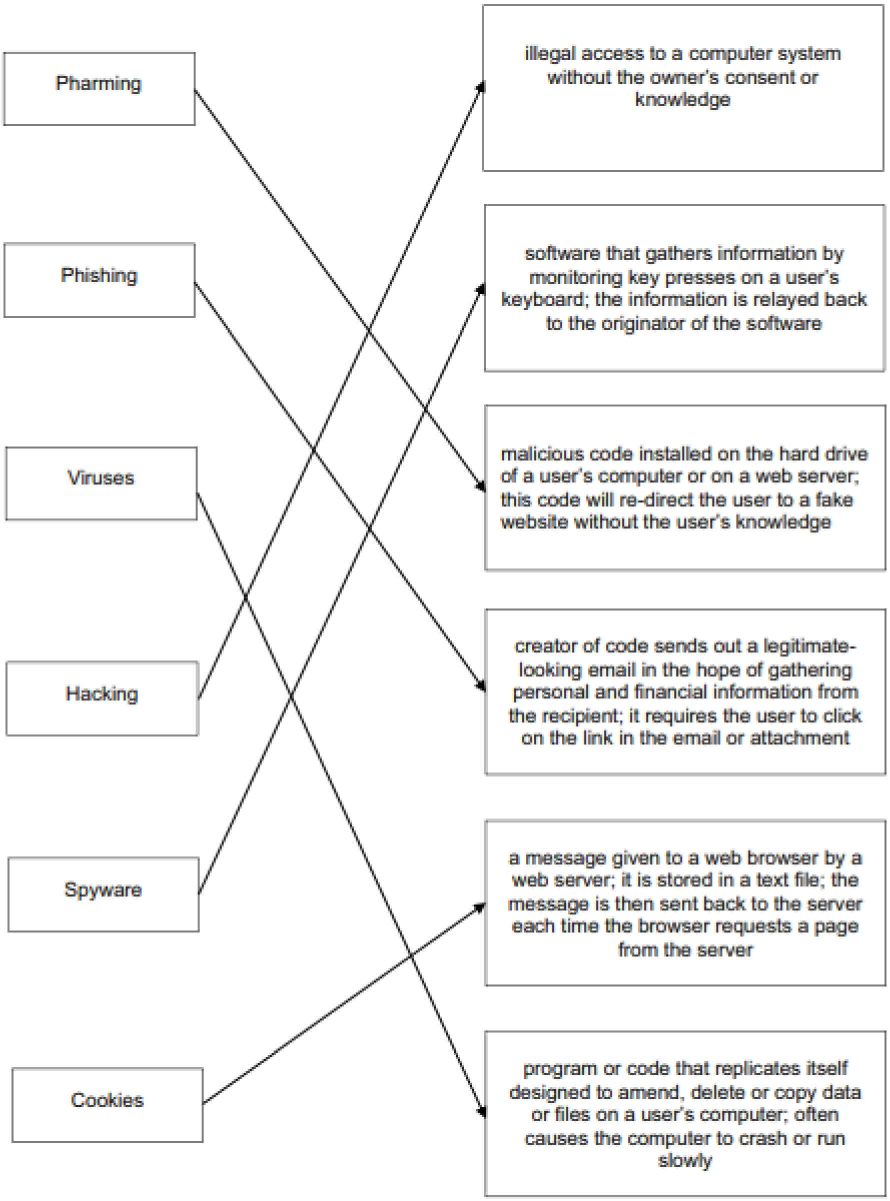
(a) Any **one** from:

– protocol ends in "s"
– use of http**<u>s</u>** [1]

(b) Any **three** 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
– if website is not secure browser will display an open padlock/warning message [3]

Q12)



Pharming

Phishing

Viruses

Hacking

Spyware

Cookies

illegal access to a computer system without the owner's consent or knowledge

software that gathers information by monitoring key presses on a user's keyboard; the information is relayed back to the originator of the software

malicious code installed on the hard drive of a user's computer or on a web server; this code will re-direct the user to a fake website without the user's knowledge

creator of code sends out a legitimate-looking email in the hope of gathering personal and financial information from the recipient; it requires the user to click on the link in the email or attachment

a message given to a web browser by a web server; it is stored in a text file; the message is then sent back to the server each time the browser requests a page from the server

program or code that replicates itself designed to amend, delete or copy data or files on a user's computer; often causes the computer to crash or run slowly

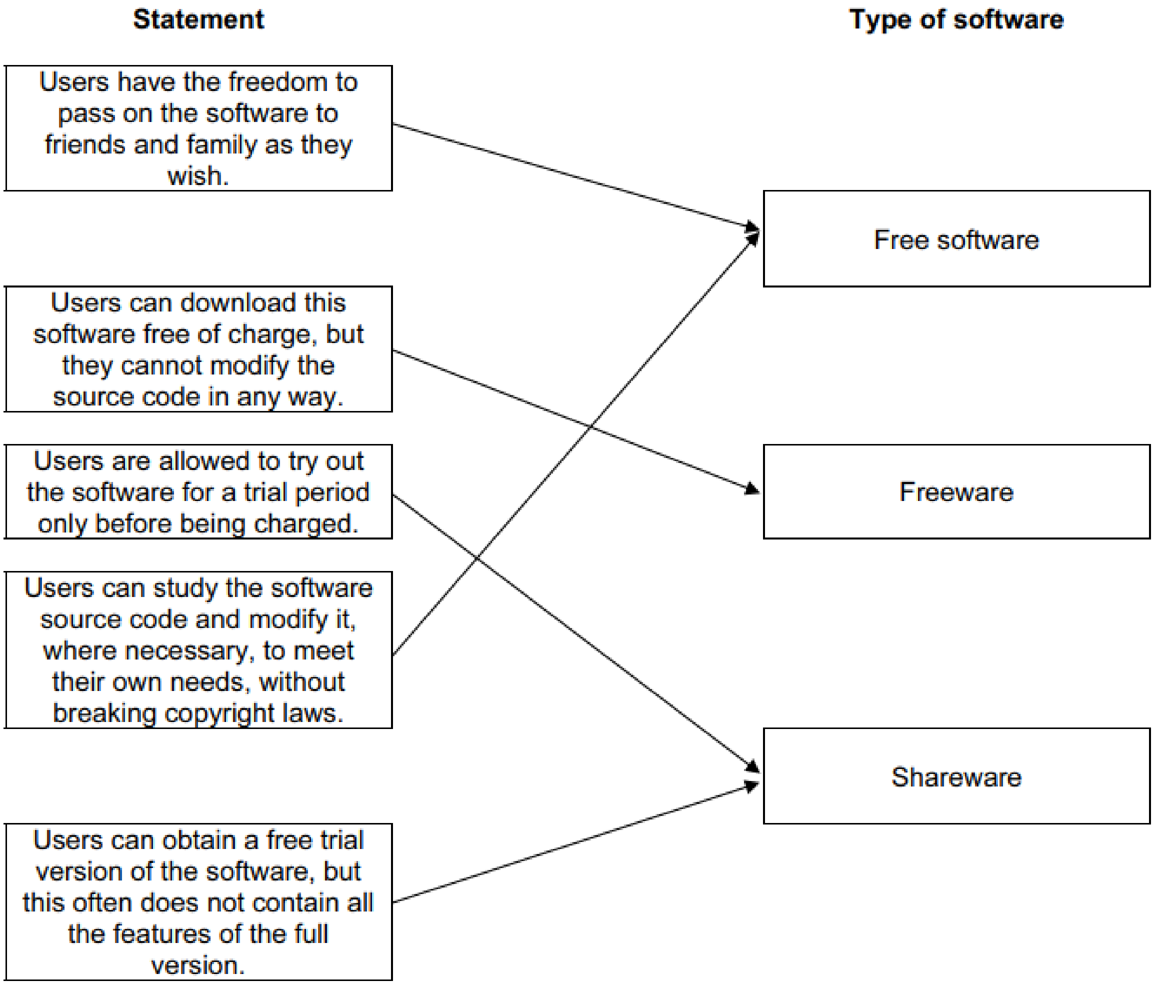
5/6 matches – 5 marks
4 matches – 4 marks
3 matches – 3 marks
2 matches – 2 marks
1 match – 1 mark

[5]

Q13)

(a) **1** mark for correct lines from each type of software

NOTE: all statements that are correct must be connected to the correct type of software for the mark to be awarded



Statement

Users have the freedom to pass on the software to friends and family as they wish.

Users can download this software free of charge, but they cannot modify the source code in any way.

Users are allowed to try out the software for a trial period only before being charged.

Users can study the software source code and modify it, where necessary, to meet their own needs, without breaking copyright laws.

Users can obtain a free trial version of the software, but this often does not contain all the features of the full version.

Type of software

Free software

Freeware

Shareware

[3]

(b) Any **three** from:

- That we should follow Copyright laws/intellectual property rights/work should not be stolen/plagiarised
- That we should follow Data Protection laws
- That we should not create or distribute malware//description of malware
- That we should not hack/crack other computers//description of hacking
- That we should protect our own computers against malware/hacking
- That we should consider privacy issues (when using social networking)
- That we consider anonymity issues (when using social networking)
- That we should consider environmental impacts when using computers
- Loss/creation of jobs from use of computers/robotics
- We should follow codes of practice (for creation of code e.g. ACM/IEEE) [3]

(c) **2** marks for each term described

Viruses:

- program/software/file that replicates (copies) itself
- intends to delete or corrupt files//fill up hard disk space

Pharming:

- malicious code stored on a computer/web server
- redirects user to fake website to steal user data

Spyware:

- monitors and relays user activity e.g. key presses//key logging software
- user activity/key presses can be analysed to find sensitive data e.g. passwords [6]

(d) Any **three** from:

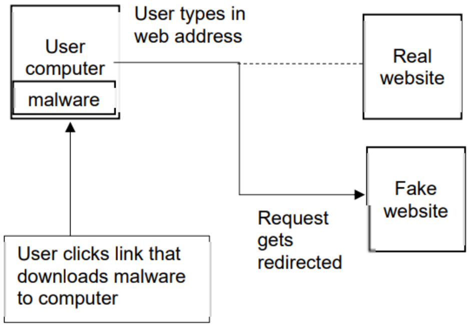
- examines/monitors traffic to and from a user's computer and a network/Internet
- checks whether incoming and outgoing traffic meets a given set of criteria/rules
- firewall blocks/filters traffic that doesn't meet the criteria/rules
- logs all incoming and outgoing traffic
- can prevent viruses or hackers gaining access
- blocks/filters access to specified IP addresses/websites
- warns users of attempts by software (in their computer) trying to access external data sources (e.g. updating of software) etc. // warns of attempted unauthorised access to the system [3]

Q14)

Question	Answer	Marks
(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	**3**
(b)(i)	Any **two** from: e.g. • Steal/view/access data • Delete data • Change data • Lock account // Encrypt data • Damage reputation of a business	**2**

Question	Answer	Marks
(b)(ii)	Any **three** from: e.g. • Virus • Worm • Trojan horse • Spyware • Adware • Ransomware	**3**
(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	**2**

Q15)

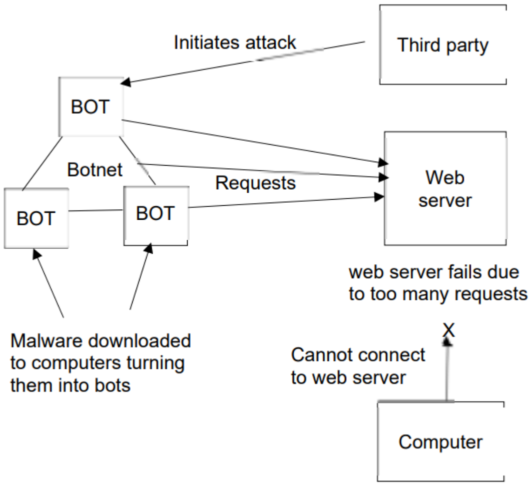
Question	Answer	Marks
(a)	• To obtain **personal** data/details // by example	**1**
(b)	**One** mark for each correct part of the diagram. Diagram shows: • User clicks/opens attachment/link that triggers download • Malicious software downloaded onto user's computer • User enters website address • User is **redirected** to fake website e.g.  User computer malware User types in web address Real website Fake website Request gets redirected User clicks link that downloads malware to computer	**4**

Q16)

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>(a)</td><td>

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


Initiates attack
Third party
BOT
Botnet
BOT
BOT
Requests
Web server
web server fails due to too many requests
X
Malware downloaded to computers turning them into bots
Cannot connect to web server
Computer

</td><td>6</td></tr>
<tr><td>(b)</td><td>

Any **two** from:
e.g.

- Revenge
- To affect a company's reputation
- Entertainment value
- To demand a ransom to stop it
- To test a system's resilience

</td><td>2</td></tr>
<tr><td>(c)</td><td>

Any **two** from:

- Proxy server
- Firewall
- Users scanning their computers with anti-malware

</td><td>2</td></tr>
</table>

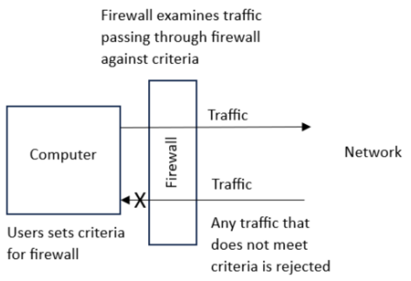
Q17)

Question	Answer	Marks
(a)	Any **three** from: e.g. • Checking the spelling and tone of the email/website • Checking the URL attached to a link • Scanning a download with anti-malware • Only downloading data / software from trusted sources • Never providing personal details online • Install a firewall to check if the website is valid	**3**
(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	**3**
(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	**3**

Q18)

Question	Answer	Marks
	One mark for each correct term in the correct order: • Malware • Bot • Botnet • Web server • Website	**5**

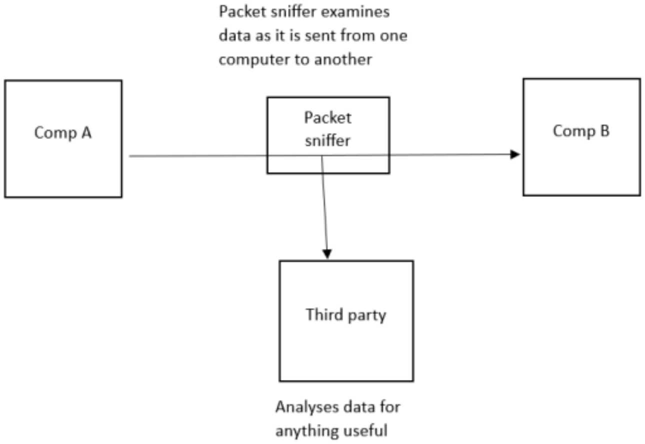
Q19)

Question	Answer	Marks
	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.  Firewall examines traffic passing through firewall against criteria Computer Firewall Traffic Network Traffic X Users sets criteria for firewall Any traffic that does not meet criteria is rejected	**4**

Q20)

Question	Answer	Marks
(a)	– A	1
(b)	Any **one** from: – Spyware // Keylogger – Adware – Trojan horse	1
(c)	– Anti-malware	1

Q21)

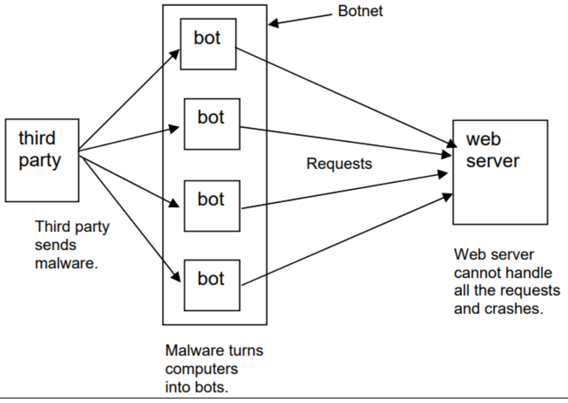
Question	Answer	Marks
(a)	The diagram demonstrates (**One** mark for each part of the diagram): – Data is being sent from one device to another – The data is being examined **during transmission** – Packet sniffer is used – Intercepted data is reported to a third-party **during transmission** … – … and analysed for anything useful – Connection hacked to spoof destination address e.g.  Packet sniffer examines data as it is sent from one computer to another Comp A Packet sniffer Comp B Third party Analyses data for anything useful	4
(b)	– Encryption … – … if the data is intercepted it will be **meaningless** (because they do not have the decryption key)	2

Q22)

(c)(i)	Any **five** from: • Criteria can be set (for traffic) • … such as a **blacklist/whitelist** (of IP addresses) • It will examine traffic coming into the network • It will check that the traffic meets the set criteria • … and will reject it if it does not meet criteria • Certain ports used by hackers can be blocked/closed	**5**

Question	Answer	Marks
(c)(ii)	Any **two** from: Example: • Virus • Worm • Trojan horse • Spyware • Adware • Ransomware	**2**

Q23)

Question	Answer	Marks
(a)	**One** mark for each part of the diagram that shows: • A perpetrator/third party sending malware // user downloads/installs malware • Each computer is turned into a bot… • … to create a botnet • Third party initiates the attack • **All** the bots send a request at once to a **web server** • … crashing the webserver Example:  Botnet bot bot bot bot third party Requests web server Third party sends malware. Web server cannot handle all the requests and crashes. Malware turns computers into bots.	**5**
(b)	Proxy server	**1**

Q24)

Question	Answer	Marks
(d)(i)	Any **three** from: • DDoS // DoS • Hacking • Malware // by example • Brute-force attack NOTE: three different examples of malware can be awarded.	**3**
(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	**2**
(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	**6**