MARK SCHEME

CAMBRIDGE INTERNATIONAL EDUCTION 0478/0981

Feb/March 2022

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>5(c)</td><td>1 mark for threat. 1 for impact. 1 for software.

Do not award identical impacts twice but read whole answer and award if additional impact given.
Allow the same software twice.
e.g.
<table>
<tr><th>Threat</th><th>Impact on company</th><th>Software</th></tr>
<tr><td>Denial of service</td><td>• Users cannot access the website
• Loss of sales (of holidays)
• Loss of reputation</td><td>Proxy/firewall</td></tr>
<tr><td>Virus/malware</td><td>• Data on the server may be deleted/changed
• Website may be deleted/changed
• Server may be filled with data and crash</td><td>Anti-virus</td></tr>
<tr><td>Unauthorised access // hacker</td><td>• Data could be deleted/stolen/changed</td><td>Proxy/Firewall</td></tr>
</table></td><td>6</td></tr>
</table>

Feb/March 2021

Question	Answer	Marks
6(a)	Any **four** from: – Monitors incoming and outgoing traffic – Allows the **setting** of criteria/blacklist/whitelist/by example – Blocks access to signals that do not meet requirements/criteria/blacklist/whitelist … – … sends signal to warn the user – Restrict access to specific applications – Blocks entry/exit by specific ports	**4**
6(b)	**One** mark for risk, **two** marks for description – Phishing – **Legitimate looking email** sent to user – Clicking on **link/attachment** takes user to fake website – Pharming – Software is installed on user's computer – Redirects (correct URL) to different/fraudulent website – Spyware (accept keylogger but do not award for MP3) – Software is installed on user's computer – Records key strokes // keylogger – Transmits data to third part for analysis	**6**

May/June 2021 V1

Question	Answer	Marks
3(a)	One mark per each correct term in the correct order. – Software – Network – Criteria – Accept // reject – Reject // accept – Hacking	**6**

Question	Answer	Marks
3(b)	Any **three** from: – Password – Biometrics (device) – Encryption – Physical methods (e.g. locks) – Two-factor authentication // Two-step verification – Anti-viruses	**3**

Question	Answer	Marks
4	Any **six** from: Phishing – Legitimate looking email sent to user – encourages user to **click a link** that directs user to a fake website – User encouraged to enter personal details into a fake website // designed to obtain personal details from a user Pharming – Malicious code/malware is downloaded/installed // software downloaded without users' knowledge – … that **re-directs** user to fake website (when legitimate URL entered) – User encouraged to enter personal details into a fake website // designed to obtain personal details from a user	**6**

May/June 2021 V2

<table>
<tr><th>Question</th><th>Answer</th><th>Marks</th></tr>
<tr><td>4(a)</td><td>One mark per each correct row.

<table>
<tr><th>Statement</th><th>Virus (✓)</th><th>Spyware (✓)</th><th>Denial of service (✓)</th></tr>
<tr><td>captures all data entered using a keyboard</td><td></td><td>✓</td><td></td></tr>
<tr><td>can be installed onto a web server</td><td>✓</td><td>✓</td><td></td></tr>
<tr><td>prevents access to a website</td><td></td><td></td><td>✓</td></tr>
<tr><td>is malicious code on a computer</td><td>✓</td><td>✓</td><td></td></tr>
<tr><td>is self-replicating</td><td>✓</td><td></td><td></td></tr>
<tr><td>damages the files on a user's hard drive</td><td>✓</td><td></td><td></td></tr>
</table></td><td>6</td></tr>
<tr><td>4(b)</td><td>Any three from:
– Phishing
– Pharming
– Hacking // cracking</td><td>3</td></tr>
<tr><td>4(c)</td><td>Any three from:
– Human error
– Power failure/surge
– Hardware failure
– Software failure
– Fire
– Flood</td><td>3</td></tr>
</table>

May/June 2021 V3

Question	Answer	Marks
4(a)	– Legitimate looking/fake email sent to user – … that contains a link to a fake website – User **clicks link** and enters personal details (into fake website)	**3**
4(b)	Any **two** from: – Pharming – Spyware – Hacking/cracking	**2**

May/June 2020 V2

Question	Answer	Marks
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	**3**
10(b)	– Virus – Malware	**2**
10(c)(i)	– Incorrect	**1**
10(c)(ii)	Any **four** from: – Can help prevent hacking – Can monitor incoming and outgoing traffic – Can set criteria / rules are set for traffic – Can check whether traffic meets / defies criteria rules – Can rejects any traffic that does not meet / defies criteria	**4**

May/June 2020 V3

Question	Answer	Marks
7(a)	Any **four** from: – Examines outgoing traffic to check what is being requested – Examines incoming traffic to check the content of what is being received – Sets rules/criteria for websites that can/cannot be accessed // creates a blacklist – Check if traffic meets/does not meet rules/criteria – If it does/does not, access to website granted/denied	**4**
7(b)	Any **three** from: – Software that can replicate itself – It could cause the computer to crash / run slow / generate errors – It could delete/damage files – It could fill up the storage space – It could stop the hardware being able to communicate – It could spread to other devices on the network	**3**

Question	Answer	Marks
7(c)(i)	Any **two** from: – Locked padlock – HTTPS – View the certificate	**2**
7(c)(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	**4**

October/November 2020 V1

5(b)	- Firewall - Proxy server	2

Feb/March 2019

Question	Answer	Marks
7	For each of **three** risks Naming the risk – 1 mark, describing the risk – 1 mark: – Hacking … – … when a person tries to gain unauthorised access to a computer system – … data can be deleted/corrupted by hacker – Malware … – … a software program designed to damage data / disrupt the computer system – … replicates itself and fills the hard disk – Virus … – … a program that replicates itself to damage / delete files NOTE: Multiple kinds of malware can be awarded if listed and given a matching description e.g. trojan horse, worm.	**6**

May/June 2019 V1

PUBLISHED

Question	Answer	Marks
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	**3**

PUBLISHED

Question	Answer	Marks
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	**3**

Question	Answer	Marks
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)**	**3**
4(b)(i)	**Three** from: • Human error e.g. accidentally deleting a file • Hardware failure • Physical damage e.g. fire/flood • Power failure // power surge • Misplacing a storage device	**3**

Question	Answer	Marks
4(b)(ii)	**Two** from: • Back data up • Use surge protection • Keep data in a fireproof / waterproof / protective case • Use verification methods (for deleting files) • Following correct procedure e.g. ejecting offline devices / regularly saving	**2**

Question	Answer	Marks
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	**4**

May/June 2019 V2

Question	Answer	Marks
5	– Password protection – **Password** is released on the **release date** – Encryption – Encryption **key** is released on the **release date**	**4**

6(e)(i)	**Four** from: – Designed to deny people access to a website – A large number/numerous requests are sent (to a server) … – … all at the same time – The server is unable to respond/struggles to respond to all the requests – The server fails/times out as a result	**4**
6(e)(ii)	**One** from: – Proxy server – Firewall	**1**

May/June 2019 V3

Question	Answer	Marks
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	**4**
3(b)	**Four** from: – An encryption algorithm is used – … to scramble data – The original data is called the plain text – A key is used to encrypt the data – The key is applied to the plain text – Plain text is encrypted into cypher text	**4**
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	**6**

October/November 2019 V1

6(b)(i)	**One** from: • Protocol is HTTPS • Padlock icon is locked • Can view website certificate	**1**
6(b)(ii)	**Five** from: • Browser / client sends request to webserver to request identification • Web server sends its digital / security certificate • Browser authenticates certificate … • … if authentic connection, is established • Any data sent is encrypted … • … using public and private keys	**5**

October/November 2019 V2

stion	Answer	Marks
(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	**3**

10(b)	**Six** from (maximum three marks per security method): • Firewall … • … Monitors the traffic • … **Blocks** any traffic that doesn't meet the **criteria** / **rules** • (Strong) password // biometric … • … Data cannot be accessed without the use of the password / bio data • … Prevent brute force attacks • Encryption … • … Data will be scrambled • … **Key** is required to decrypt the data • … If data is stolen it will be meaningless • Physical security methods … • … The physical security will need to be overcome • … This can help deter theft of the data • Antispyware … • … will remove any spyware from system • … will prevent data being relayed to a third party	**6**

October/November 2019 V3

Question	Answer	Marks
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	**4**

February/March 2018

Question	Answer	Marks
2(a)	Any **three** from: Scans files for viruses // detects/identifies a virus Can constantly run in background Can run a scheduled scan Can automatically updating virus definitions Can quarantine a virus Can delete a virus Completes heuristic checking Notifies user of a possible virus	**3**

Question	Answer	Marks
2(b)	Any **three** from: Use a firewall Use of a proxy server Do not use / download software / files from unknown sources Do not share external storage devices / USB pens Do not open / take care when opening attachments / link Do not connect computer to network / use as stand-alone computer Limiting access to the computer	**3**

May/June 2018 V1

Question	Answer	Marks
10(d)	Any **four** from: – Prevents direct access to the **webserver** // Sits between **user** and **webserver** – If an attack is launched it hits the proxy server instead // can be used to help prevent DDOS // help prevent hacking of **webserver** – Used to direct invalid traffic away from the webserver – Traffic is examined by the proxy server // Filters traffic – If traffic is valid the data from the webserver will be obtained by the user – If traffic is invalid the request to obtain data is declined – Can block requests from certain IP addresses	**4**

May/June 2018 V3

Question	Answer	Marks
3	2 marks per issue from: Phishing – Legitimate looking emails sent to use – When user clicks on attachment / link sent to fraudulent website – Asked to reveal/designed to steal sensitive information Pharming – Malicious code loaded on user hard drive – Will redirect URL requests to fraudulent website – Asked to reveal/designed to steal sensitive information Spam – Junk / unwanted email – Sent to large numbers of people – Used for advertising / spreading malware – Fills up mail boxes	**6**
4(c)(i)	– Encrypted text is meaningless – Need the key to decrypt the text	**2**
4(c)(ii)	– Increase length / more bits used for key … – … will generate more possibilities for key / less chance of decryption by brute force method	**2**

October/November 2018 V1

Question	Answer	Marks
4(a)	**Four** from: Phishing: • A legitimate looking email is sent to a user • The email will encourage the user to click a link/open an attachment • The link will redirect a user to a legitimate looking webpage (to steal personal data) Pharming: • A malicious code is installed on a user's hard drive/server • The code will cause a redirection to a legitimate looking webpage (to steal personal data)	**4**
4(b)	**Two** from: • Hacking • Cracking • Virus • Denial of service • Malware • Spyware	**2**
4(c)	**Two** from: • Firewall • Proxy server • Anti-virus • Anti-malware • Anti-spyware • Username and password	**2**

October/November 2018 V2

Question	Answer	Marks
4(a)	**Three** from: • Malware • Virus // No antivirus • Denial of service • Spyware // No antispyware • Phishing // opening unknown links/emails • Pharming // opening unknown links/emails (only award once for this alternative) • Hacking/cracking/unauthorised access // No/weak password // No/weak firewall • Downloading/Using unknown software • Not updating software • Physical issue e.g. computer/door left unlocked	**3**
4(b)	**Four** from: • It examines/monitors/filters traffic into **and** out of a computer • It allows a user to set criteria/rules for the traffic • It checks whether the traffic meets the criteria/rules • It blocks any traffic that does not meet the criteria/rules // Blocks unauthorised access • It warns a **user** of any unauthorised software/access/unauthorised outgoing traffic • It keeps a log of all traffic (that can be examined)	**4**

October/November 2018 V3

Question	Answer	Marks
6	1 mark for method name, 1 mark for description e.g. **Backups** • Make a copy of the data • Copy stored away from main computer • Data can be restored from backup **Anti-virus** • Scans computer for viruses • Software to detect/remove viruses • Can prevent data being corrupted by viruses **Firewall** • Hardware or software that monitors network traffic • To help prevent hackers gaining access / deleting data **Password/Biometrics** • To help protect files / computer from unauthorised access **Restricted access** • To stop users downloading/installing software that could harm **Verification** • Message e.g. to ask if definitely want to delete **Physical methods** • Locks/alarms/CCTV to alert/deter unauthorised access	**6**

February/March 2017

Question	Answer	Marks
4(a)	• a v m v e q n d i z m h (2 marks, 1 for each correct word)	**2**
4(b)	v w x y z a b c d e f g h i j k l m n o p q r s t u **2** marks • shift right • all characters shifted five places	**2**
4(c)	• the first cypher • cannot deduce rest of cypher having identified some characters/more random substitution	**2**

May/June 2017 V2

Question	Answer	Marks
8(a)	2 marks for SSL, 2 marks for Firewall **SSL protocol** **Two** from: ∞ uses encryption ∞ encryption is asymmetric / symmetric / both ∞ makes use of (public and private) keys ∞ data is meaningless (without decryption key / if intercepted) **Firewall** **Two** from: ∞ helps prevent unauthorised access // helps prevent hacking ∞ checks that data meets criteria // identifies when data does not meet criteria ∞ acts as a filter for (incoming and outgoing) data // blocks any unacceptable data //allows acceptable data through	**4**

Question	Answer	Marks
8(b)	**Six** from: Encrypt the data … … so it cannot be understood by those not entitled to view it Password protected / biometrics … … to help prevent unauthorised access Virus checking software … … helps prevent data corruption or deletion … identifies / removes a virus in the system … scans a system for viruses Spyware checking software … … helps prevent data being stolen/copied/logged … scans a system for spyware Drop-down input methods / selectable features … … to reduce risk of spyware / keylogging Physical method e.g. locked doors / CCTV timeout / auto log off … to help prevent unauthorised access Network / company policies // training employees … to educate users how to be vigilant Access rights … … allows users access to data that they have permission to view … prevents users from accessing data that they do not have permission to view	**6**

October/November 2017 V1

Question	Answer	Marks
8(a)	Any **three** from: – Human error (e.g. deleting/overwriting data) – Physical damage – Power failure/surge – Hardware failure – Software crashing	**3**
8(b)	Any **three** from: – Online shopping // Online payment systems // Online booking – Email – Cloud based storage – Intranet/extranet – VPN – VoIP // video conferencing – Instant messaging (IM) // social networking // online gaming	**3**

Question	Answer	Marks
8(c)	1 mark for identifying, 1 mark for description – Strong password – To make it difficult to hack an account – Biometric device – To use data that is difficult to fake as a password – TLS // Encryption – To make data meaningless if intercepted – To encrypt data that is exchanged (TLS only) – More secure than SSL (TLS only) – Anti-spyware (software) – To find and remove any spyware that is installed on a computer – To help stop key loggers recording key presses – Firewall – To help prevent unauthorised access to an account – Blocks any requests that do not meet/match the criteria – Authentication (card reader at home)/mobile security code app/two-step verification – To add another level of identification of the user – Use of drop-down boxes (or equivalent) – So key loggers cannot record the key presses – Proxy server – To divert an attack away from the main system	**6**

October/November 2017 V2

Question	Answer	Marks
10(a)	Any **three** from: ∞ It is a (security) protocol ∞ It encrypts data (sent over the web/network) ∞ It is the updated version of SSL ∞ It has two layers ∞ It has a handshake layer ∞ It has a record layer	**3**
10(b)	1 mark for each correct application, examples could include: ∞ Online banking ∞ Online shopping // Online payment systems ∞ Email ∞ Cloud based storage ∞ Intranet/extranet ∞ VPN ∞ VoIP ∞ Instant messaging (IM) // social networking	**3**

Question	Answer	Marks
11	1 mark for each correct missing word, in the correct order: ∞ Plagiarism ∞ Free software ∞ Freeware ∞ Shareware ∞ Ethics	**5**

May/June 2016 V1

6 **(a)** Any **one** from:

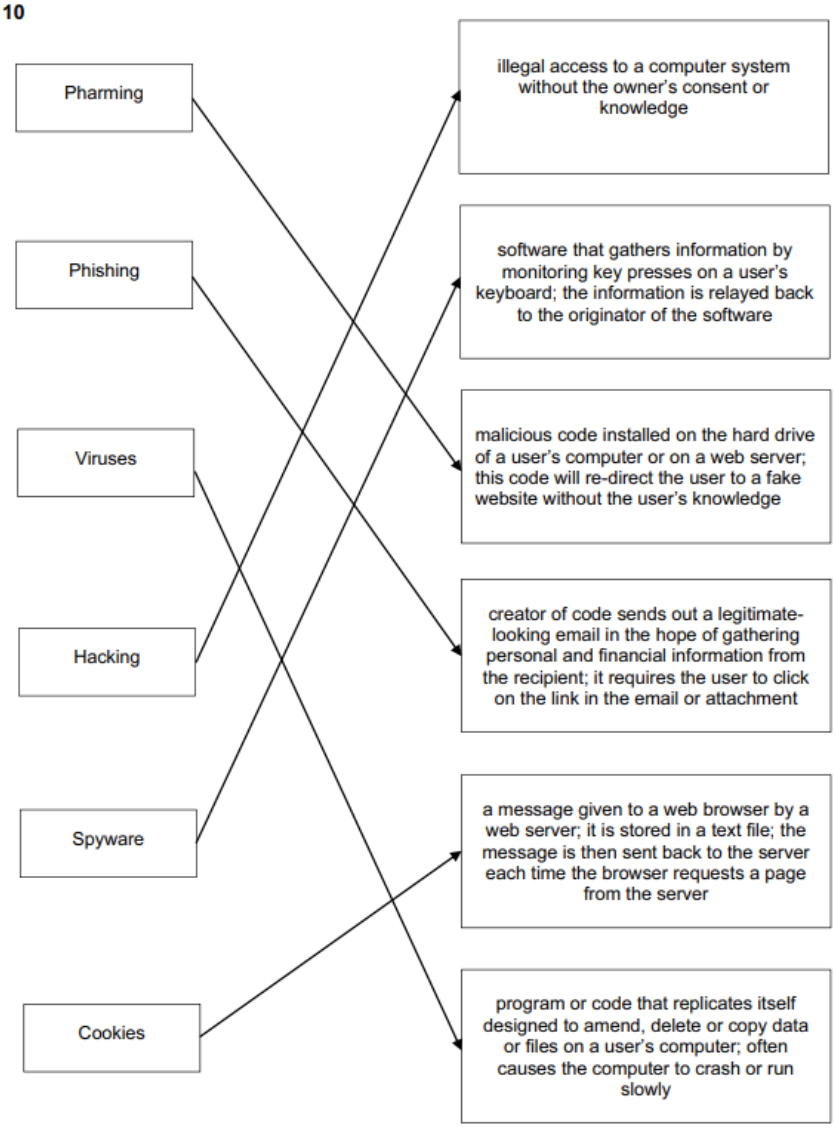
- protocol ends in “s”
- use of http**s**

[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

10



ng message [3]

May/June 2016 V2

(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]

October/November 2016 V1

2
- Hacking
- Virus
- Cookies
- Cracking
- Pharming [5]

(c) 1 mark for security measure, 1 mark for description.

Any **two** from:

- Encryption
- If the data is accessed or stolen it will be meaningless

- Biometric device
- Can help prevents unauthorised access to the system (only award once)

- Firewall
- Can alert to show unauthorised access attempt on the system
- Can help prevent unauthorised access to the system (only award once)
- Can help protect against viruses and malware entering the system

- Anti-spyware
- Can stop the keys being logged that, when analysed, would reveal the password to the data [4]

October/November 2016 V2

9 **(a)** Any **two** from:

- a large number of requests are sent to the network/server all at once
- designed to flood a network/server with useless traffic/requests
- the network/server will come to a halt/stop trying to deal with all the traffic/requests
- prevents users from gaining access to a website/server

[2]

(b) 1 mark for each security threat and 1 mark for matching description

Security threat	**Description**
Viruses	– software that replicates – causes loss/corruption of data // computer may "crash"/run slow
Hacking/cracking	– illegal/ unauthorised access to a system/data
Phishing	– a link/attachment sends user to fake website (where personal data may be obtained)
Pharming	– malicious code installed on user's hard drive / computer – user is redirected to a fake website (where personal data may be obtained)
Spyware/key logger	– send/relay key strokes to a third party

[4]