MODULE G SECURITY · G7

Firewalls, anti-malware and updates: mark scheme

21 marks · Cambridge 0478 syllabus 5.3.2 (explain how a range of solutions are used to help keep data safe from security threats: anti-malware, including anti-virus and anti-spyware; automating software updates; firewalls)

How to use. One mark per creditworthy point up to the maximum shown. **/** separates alternative words; **//** separates alternative answers. Words in (brackets) are not needed for the mark. **...** at the start of a point means it builds on the point before. Credit any other valid answer that shows the same understanding. Access levels, authentication, proxy-servers, privacy settings, SSL and checking URLs / communications (also 5.3.2) are tested in other Module G worksheets, not here.

QUESTION	ANSWER	MARKS	GUIDANCE
1(a) 0478 5.3.2	Installs patches as soon as they are released: Automating software updates Checks traffic between a network and the internet against rules: Firewall Finds and removes software that records key presses: Anti-spyware Scans files and compares them with known viruses: Anti-virus	**4**	One mark per correct row. A row with more than one tick scores 0.
2(a) 0478 5.3.2	Any three from: Monitors / examines (all) the traffic coming into (and going out of) the network Checks whether the traffic meets the rules / criteria (set by the network manager) Blocks / rejects traffic that does not meet the rules // traffic from a blacklisted / unknown source Allows traffic that meets the rules // traffic from a whitelisted / trusted source Can block traffic from hackers // unauthorised access to the server // traffic that may carry malware Can keep a log of (blocked) traffic // alert the network manager	**3**	max 3. "Stops hackers" alone is too vague: it must be linked to blocking traffic. Do not credit scanning files for viruses (that is anti-virus).
2(b) 0478 5.3.2	Any two from: Block traffic from a particular / suspicious IP address // set a blacklist of IP addresses Only allow traffic from trusted / known IP addresses // set a whitelist Block access to particular websites / URLs Block particular ports // types of traffic // applications from using the network Block incoming traffic that was not requested by a computer on the network Block traffic at certain times // outside office hours	**2**	max 2. The same rule given twice in different words scores 1. "Block bad / dangerous traffic" alone is too vague.

QUESTION	ANSWER	MARKS	GUIDANCE
3(a) 0478 5.3.2	Any three from: Scans the computer system / files (for viruses) Has a record / database of known viruses // compares files with known viruses Checks files / data before they are downloaded / opened // scans in real time ... and stops the download // warns the user the file may contain a virus Quarantines / removes / deletes any virus found ... so the virus cannot replicate / spread // delete or corrupt the firm's data Can run scheduled / regular scans	**3**	max 3. "Gets rid of viruses" alone scores 1 (removes any virus found) only.
3(b) 0478 5.3.2	Any one from: Scans the computer for spyware Removes / quarantines any spyware that is found Stops spyware being downloaded / installed Stops spyware recording key presses // sending the financial details to a third party	**1**	Do not credit answers about viruses only, or "stops hacking".
3(c) 0478 5.3.2	Any two from: New malware / viruses / spyware are created all the time ... the update adds them to the record / database of known malware ... otherwise new malware would not be detected / removed // could infect the computers Updates can fix weaknesses / bugs in the anti-malware software itself	**2**	max 2. "To keep it up to date" alone is too vague.
4(a) 0478 5.3.2	Any three from: Updates contain patches // fix bugs / security weaknesses / vulnerabilities in the software ... that hackers / malware could use to gain access to the computers / data Automatic updates are installed as soon as they are released ... so the computers are open to attack for less time Does not rely on staff remembering / choosing to install updates // staff cannot delay or ignore them All computers are kept up to date (with the latest version) Anti-malware updates are also installed automatically // new malware can be detected straight away	**3**	max 3. "Keeps the software up to date" alone scores 0 unless linked to fixing weaknesses or speed of installation. Do not credit "updates stop all attacks".

QUESTION	ANSWER	MARKS	GUIDANCE
5(a) 0478 5.3.2	Any three from: A firewall only checks / filters the traffic between the network and the internet A firewall does not scan the files stored on the computers A firewall does not remove / quarantine malware (already on a computer) Malware can arrive in traffic that the firewall allows // in an email attachment / download from an allowed source Malware can arrive without going through the firewall // e.g. on a USB memory stick / external storage Anti-malware scans files and compares them with known malware // detects and removes malware the firewall misses The two solutions work together // give more than one layer of protection	**3**	max 3. "A firewall cannot stop viruses" alone is too vague.

Total: 21 marks