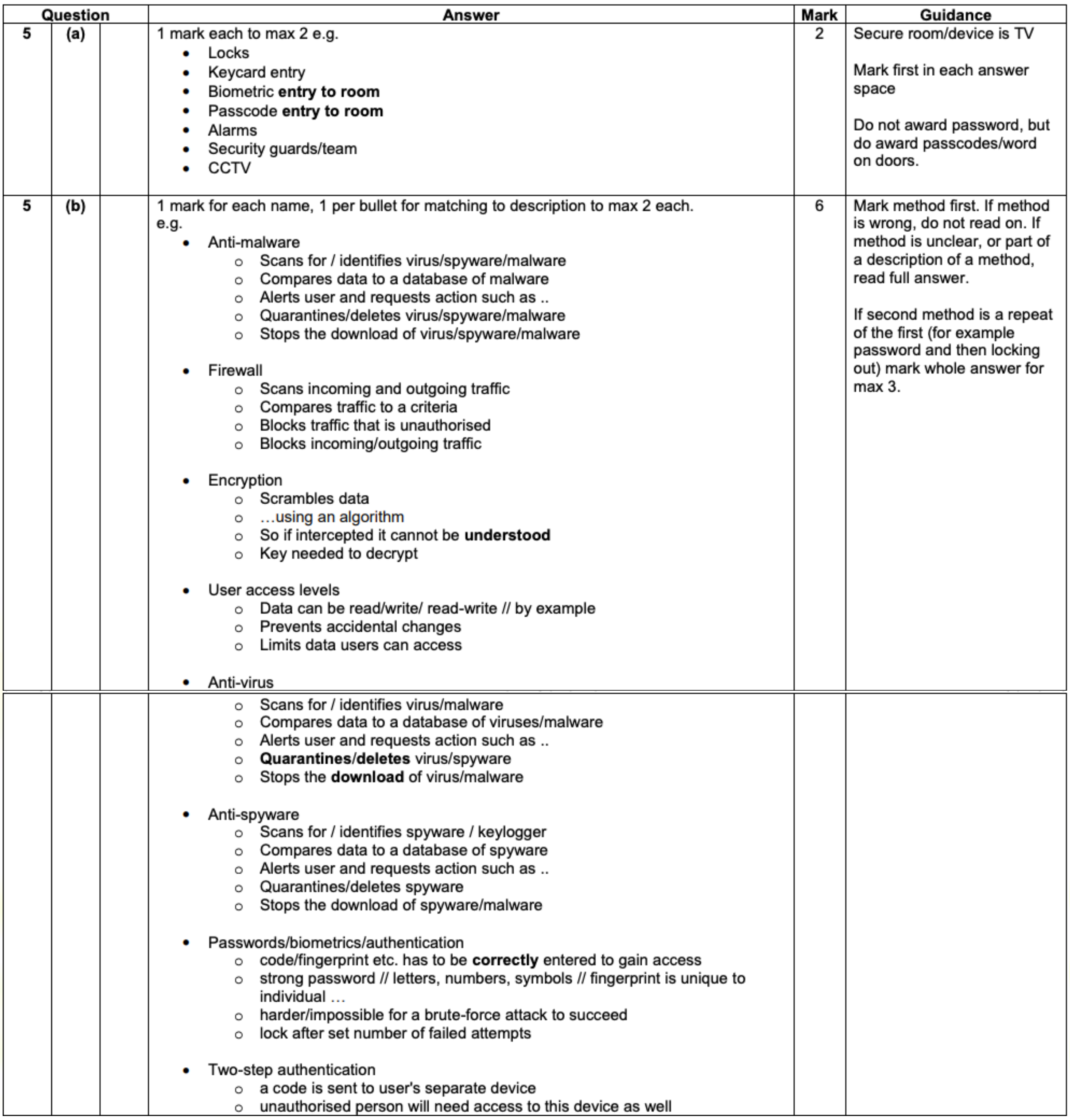
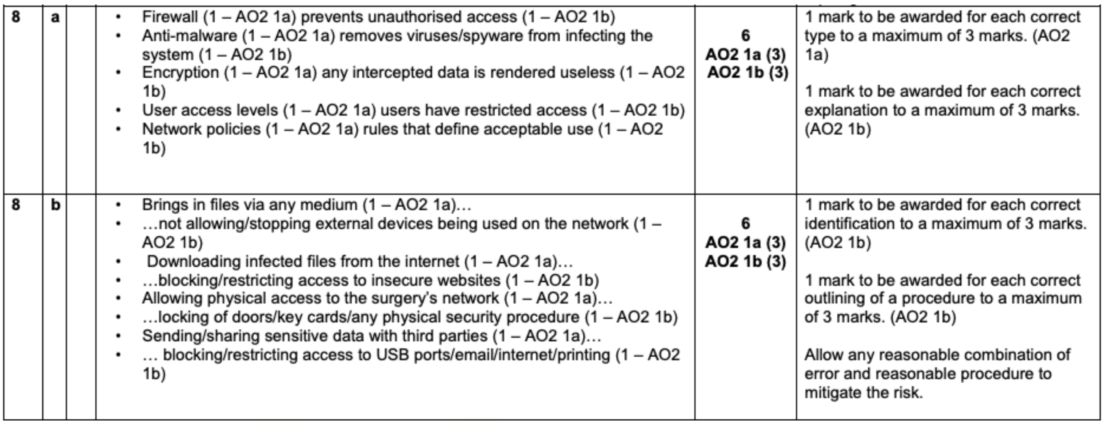
1.4 Network Security – Past Exam Questions – Solutions

2022



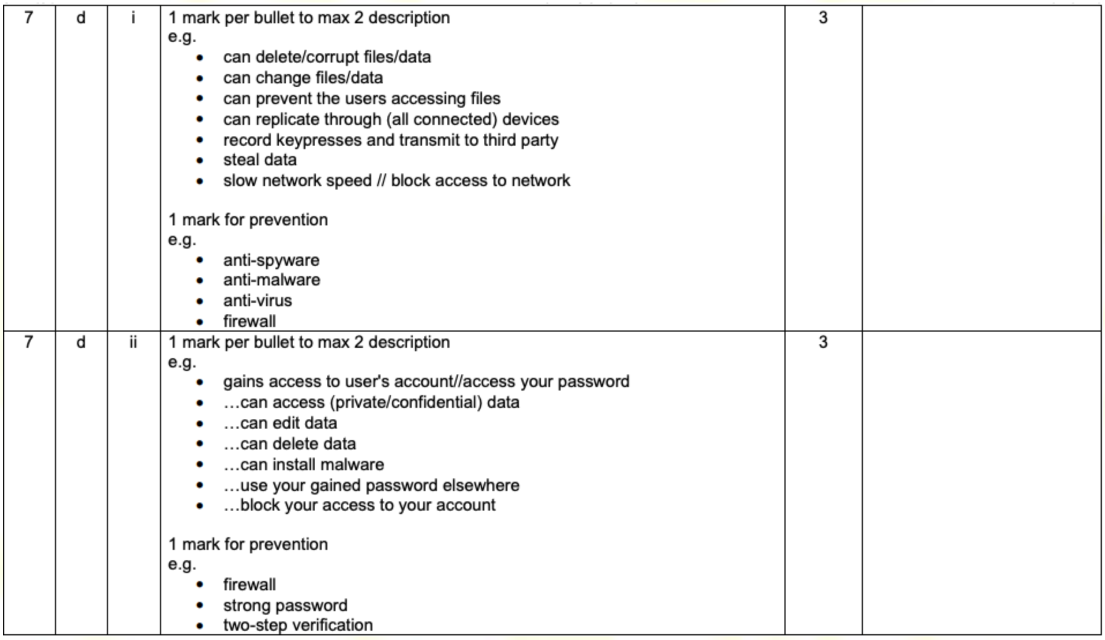
Question			Answer	Mark	Guidance
5	(a)		1 mark each to max 2 e.g. • Locks • Keycard entry • Biometric **entry to room** • Passcode **entry to room** • Alarms • Security guards/team • CCTV	2	Secure room/device is TV Mark first in each answer space Do not award password, but do award passcodes/word on doors.
5	(b)		1 mark for each name, 1 per bullet for matching to description to max 2 each. e.g. • Anti-malware ○ Scans for / identifies virus/spyware/malware ○ Compares data to a database of malware ○ Alerts user and requests action such as .. ○ Quarantines/deletes virus/spyware/malware ○ Stops the download of virus/spyware/malware • Firewall ○ Scans incoming and outgoing traffic ○ Compares traffic to a criteria ○ Blocks traffic that is unauthorised ○ Blocks incoming/outgoing traffic • Encryption ○ Scrambles data ○ …using an algorithm ○ So if intercepted it cannot be **understood** ○ Key needed to decrypt • User access levels ○ Data can be read/write/ read-write // by example ○ Prevents accidental changes ○ Limits data users can access • Anti-virus ○ Scans for / identifies virus/malware ○ Compares data to a database of viruses/malware ○ Alerts user and requests action such as .. ○ **Quarantines/deletes** virus/spyware ○ Stops the **download** of virus/malware • Anti-spyware ○ Scans for / identifies spyware / keylogger ○ Compares data to a database of spyware ○ Alerts user and requests action such as .. ○ Quarantines/deletes spyware ○ Stops the download of spyware/malware • Passwords/biometrics/authentication ○ code/fingerprint etc. has to be **correctly** entered to gain access ○ strong password // letters, numbers, symbols // fingerprint is unique to individual … ○ harder/impossible for a brute-force attack to succeed ○ lock after set number of failed attempts • Two-step authentication ○ a code is sent to user's separate device ○ unauthorised person will need access to this device as well	6	Mark method first. If method is wrong, do not read on. If method is unclear, or part of a description of a method, read full answer. If second method is a repeat of the first (for example password and then locking out) mark whole answer for max 3.

Sample Paper



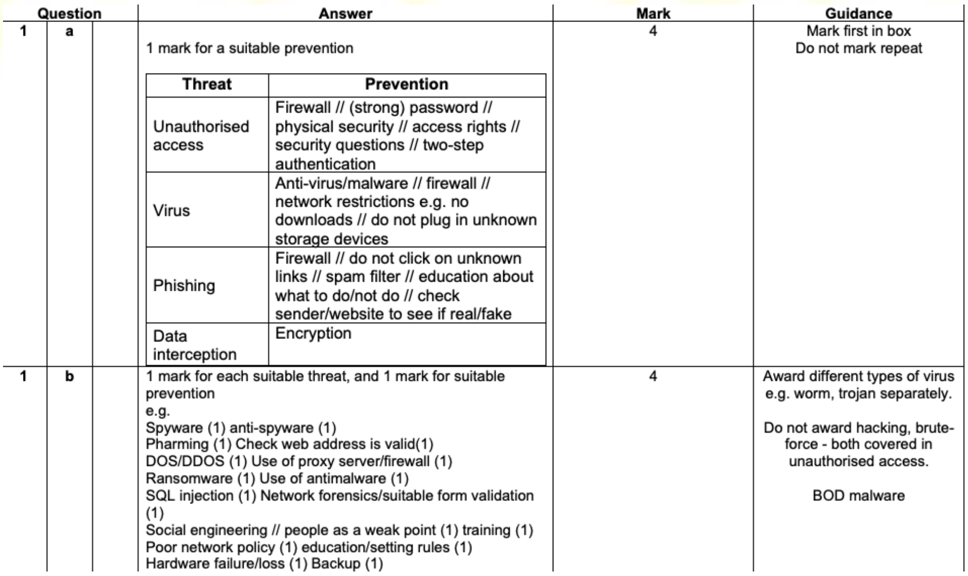
8	a		• Firewall (1 – AO2 1a) prevents unauthorised access (1 – AO2 1b) • Anti-malware (1 – AO2 1a) removes viruses/spyware from infecting the system (1 – AO2 1b) • Encryption (1 – AO2 1a) any intercepted data is rendered useless (1 – AO2 1b) • User access levels (1 – AO2 1a) users have restricted access (1 – AO2 1b) • Network policies (1 – AO2 1a) rules that define acceptable use (1 – AO2 1b)	**6** **AO2 1a (3)** **AO2 1b (3)**	1 mark to be awarded for each correct type to a maximum of 3 marks. (AO2 1a) 1 mark to be awarded for each correct explanation to a maximum of 3 marks. (AO2 1b)
8	b		• Brings in files via any medium (1 – AO2 1a)… • …not allowing/stopping external devices being used on the network (1 – AO2 1b) • Downloading infected files from the internet (1 – AO2 1a)… • …blocking/restricting access to insecure websites (1 – AO2 1b) • Allowing physical access to the surgery's network (1 – AO2 1a)… • …locking of doors/key cards/any physical security procedure (1 – AO2 1b) • Sending/sharing sensitive data with third parties (1 – AO2 1a)… • … blocking/restricting access to USB ports/email/internet/printing (1 – AO2 1b)	**6** **AO2 1a (3)** **AO2 1b (3)**	1 mark to be awarded for each correct identification to a maximum of 3 marks. (AO2 1b) 1 mark to be awarded for each correct outlining of a procedure to a maximum of 3 marks. (AO2 1b) Allow any reasonable combination of error and reasonable procedure to mitigate the risk.

2021



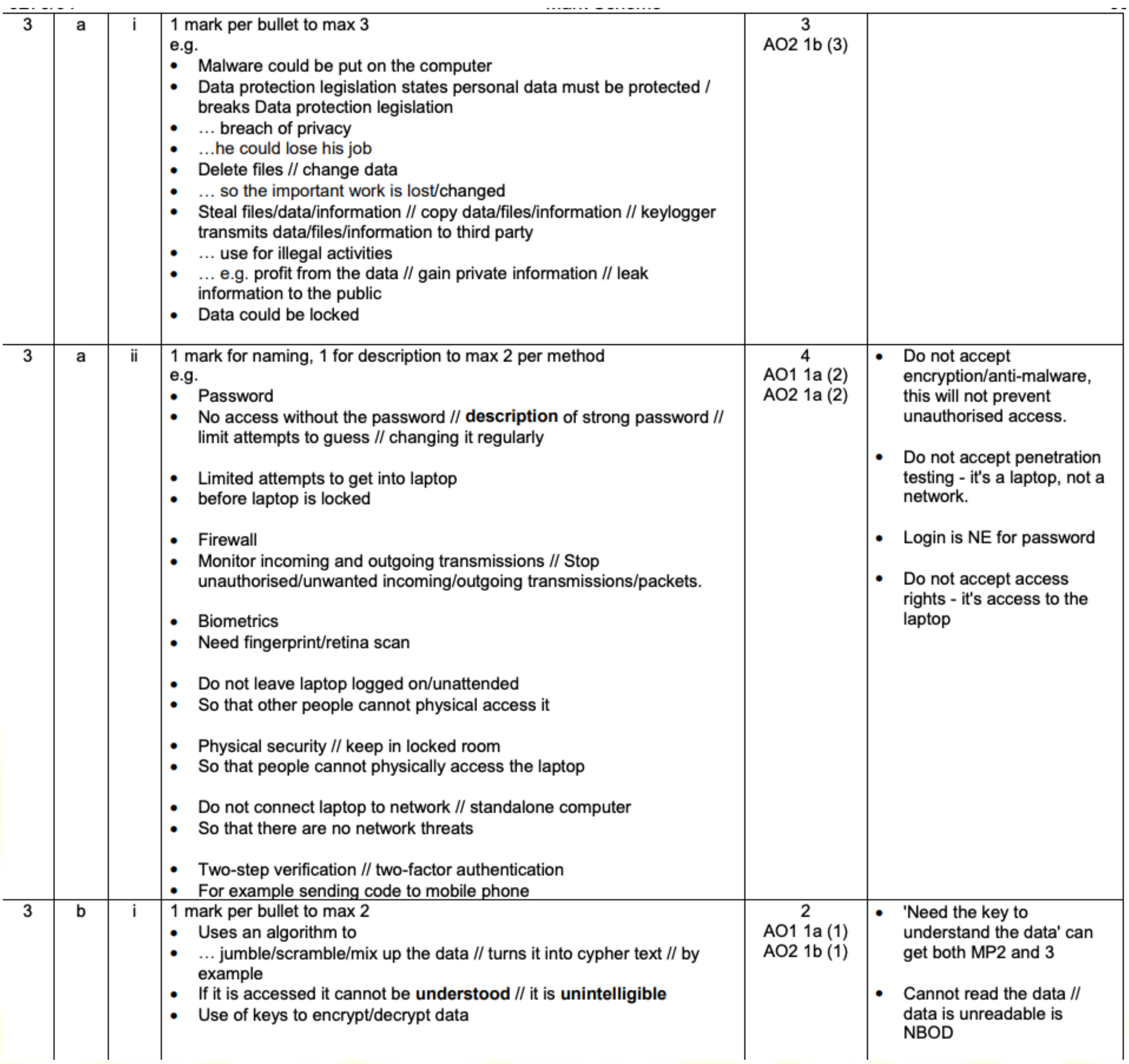
7	d	i	1 mark per bullet to max 2 description e.g. • can delete/corrupt files/data • can change files/data • can prevent the users accessing files • can replicate through (all connected) devices • record keypresses and transmit to third party • steal data • slow network speed // block access to network 1 mark for prevention e.g. • anti-spyware • anti-malware • anti-virus • firewall	3	
7	d	ii	1 mark per bullet to max 2 description e.g. • gains access to user's account//access your password • …can access (private/confidential) data • …can edit data • …can delete data • …can install malware • …use your gained password elsewhere • …block your access to your account 1 mark for prevention e.g. • firewall • strong password • two-step verification	3	

2020



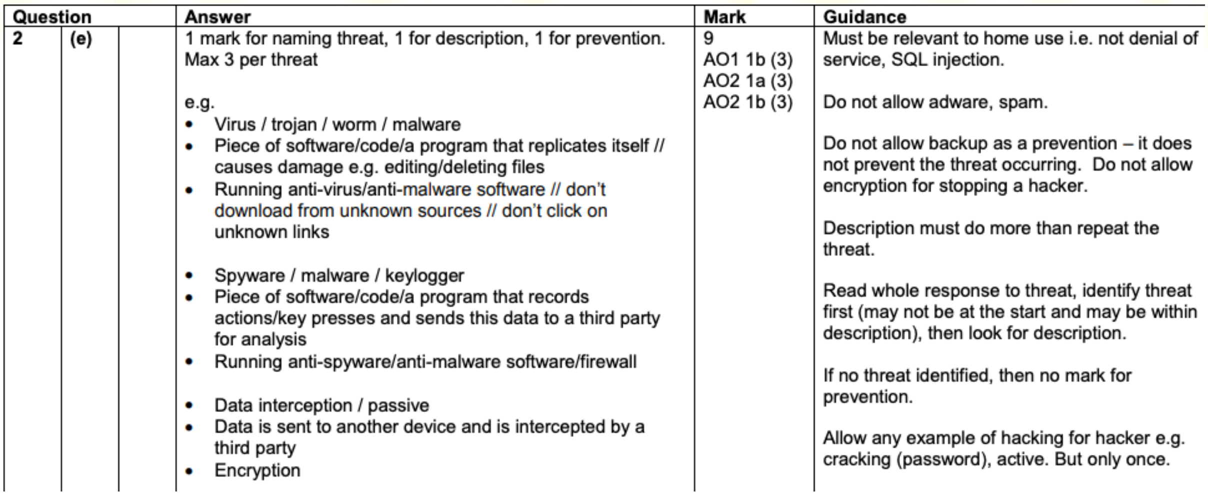
<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Mark</th><th>Guidance</th></tr>
<tr><td>1</td><td>a</td><td></td><td>1 mark for a suitable prevention
<table>
<tr><th>Threat</th><th>Prevention</th></tr>
<tr><td>Unauthorised access</td><td>Firewall // (strong) password // physical security // access rights // security questions // two-step authentication</td></tr>
<tr><td>Virus</td><td>Anti-virus/malware // firewall // network restrictions e.g. no downloads // do not plug in unknown storage devices</td></tr>
<tr><td>Phishing</td><td>Firewall // do not click on unknown links // spam filter // education about what to do/not do // check sender/website to see if real/fake</td></tr>
<tr><td>Data interception</td><td>Encryption</td></tr>
</table></td><td>4</td><td>Mark first in box
Do not mark repeat</td></tr>
<tr><td>1</td><td>b</td><td></td><td>1 mark for each suitable threat, and 1 mark for suitable prevention
e.g.
Spyware (1) anti-spyware (1)
Pharming (1) Check web address is valid(1)
DOS/DDOS (1) Use of proxy server/firewall (1)
Ransomware (1) Use of antimalware (1)
SQL injection (1) Network forensics/suitable form validation (1)
Social engineering // people as a weak point (1) training (1)
Poor network policy (1) education/setting rules (1)
Hardware failure/loss (1) Backup (1)</td><td>4</td><td>Award different types of virus e.g. worm, trojan separately.
Do not award hacking, brute-force - both covered in unauthorised access.
BOD malware</td></tr>
</table>

2019

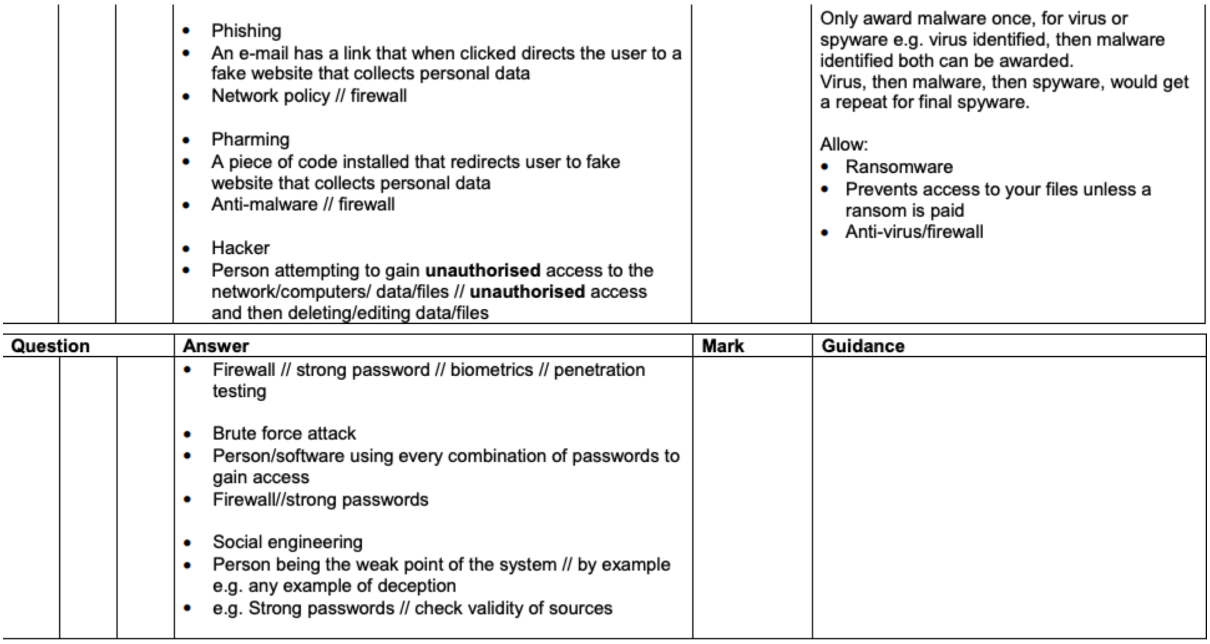


3	a	i	1 mark per bullet to max 3 e.g. • Malware could be put on the computer • Data protection legislation states personal data must be protected / breaks Data protection legislation • … breach of privacy • …he could lose his job • Delete files // change data • … so the important work is lost/changed • Steal files/data/information // copy data/files/information // keylogger transmits data/files/information to third party • … use for illegal activities • … e.g. profit from the data // gain private information // leak information to the public • Data could be locked	3 AO2 1b (3)	
3	a	ii	1 mark for naming, 1 for description to max 2 per method e.g. • Password • No access without the password // **description** of strong password // limit attempts to guess // changing it regularly • Limited attempts to get into laptop • before laptop is locked • Firewall • Monitor incoming and outgoing transmissions // Stop unauthorised/unwanted incoming/outgoing transmissions/packets. • Biometrics • Need fingerprint/retina scan • Do not leave laptop logged on/unattended • So that other people cannot physical access it • Physical security // keep in locked room • So that people cannot physically access the laptop • Do not connect laptop to network // standalone computer • So that there are no network threats • Two-step verification // two-factor authentication • For example sending code to mobile phone	4 AO1 1a (2) AO2 1a (2)	• Do not accept encryption/anti-malware, this will not prevent unauthorised access. • Do not accept penetration testing - it's a laptop, not a network. • Login is NE for password • Do not accept access rights - it's access to the laptop
3	b	i	1 mark per bullet to max 2 • Uses an algorithm to • … jumble/scramble/mix up the data // turns it into cypher text // by example • If it is accessed it cannot be **understood** // it is **unintelligible** • Use of keys to encrypt/decrypt data	2 AO1 1a (1) AO2 1b (1)	• 'Need the key to understand the data' can get both MP2 and 3 • Cannot read the data // data is unreadable is NBOD

2018



Question			Answer	Mark	Guidance
2	(e)		1 mark for naming threat, 1 for description, 1 for prevention. Max 3 per threat e.g. • Virus / trojan / worm / malware • Piece of software/code/a program that replicates itself // causes damage e.g. editing/deleting files • Running anti-virus/anti-malware software // don't download from unknown sources // don't click on unknown links • Spyware / malware / keylogger • Piece of software/code/a program that records actions/key presses and sends this data to a third party for analysis • Running anti-spyware/anti-malware software/firewall • Data interception / passive • Data is sent to another device and is intercepted by a third party • Encryption	9 AO1 1b (3) AO2 1a (3) AO2 1b (3)	Must be relevant to home use i.e. not denial of service, SQL injection. Do not allow adware, spam. Do not allow backup as a prevention – it does not prevent the threat occurring. Do not allow encryption for stopping a hacker. Description must do more than repeat the threat. Read whole response to threat, identify threat first (may not be at the start and may be within description), then look for description. If no threat identified, then no mark for prevention. Allow any example of hacking for hacker e.g. cracking (password), active. But only once.



Question			Answer	Mark	Guidance
			• Phishing • An e-mail has a link that when clicked directs the user to a fake website that collects personal data • Network policy // firewall • Pharming • A piece of code installed that redirects user to fake website that collects personal data • Anti-malware // firewall • Hacker • Person attempting to gain **unauthorised** access to the network/computers/ data/files // **unauthorised** access and then deleting/editing data/files • Firewall // strong password // biometrics // penetration testing • Brute force attack • Person/software using every combination of passwords to gain access • Firewall//strong passwords • Social engineering • Person being the weak point of the system // by example e.g. any example of deception • e.g. Strong passwords // check validity of sources		Only award malware once, for virus or spyware e.g. virus identified, then malware identified both can be awarded. Virus, then malware, then spyware, would get a repeat for final spyware. Allow: • Ransomware • Prevents access to your files unless a ransom is paid • Anti-virus/firewall