The answers on this worksheet have been taken from the 2018 OCR GCSE Computer Science Paper 1

6-A-Day – Computer Science GCSE (p1.7-2016)

Q1	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 • 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	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. 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

The answers on this worksheet have been taken from the 2018 OCR GCSE Computer Science Paper 1

Q2

Mark Band 3–High Level
(6-8 marks)
The candidate demonstrates a thorough knowledge and understanding of a wide range of considerations in relation to the question; the material is generally accurate and detailed.
The candidate is able to apply their knowledge and understanding directly and consistently to the context provided. Evidence/examples will be explicitly relevant to the explanation.
The candidate is able to weigh up both sides of the discussion and includes reference to the impact on all areas showing thorough recognition of influencing factors.
There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.

Mark Band 2-Mid Level
(3-5 marks)
The candidate demonstrates reasonable knowledge and understanding of a range of considerations in relation to the question; the material is generally accurate but at times underdeveloped.
The candidate is able to apply their knowledge and understanding directly to the context provided although one or two opportunities are missed. Evidence/examples are for the most part implicitly relevant to the explanation.
The candidate makes a reasonable attempt to discuss the impact on most areas, showing reasonable recognition of influencing factors.
There is a line of reasoning presented with some structure. The information presented is in the most part relevant and supported by some evidence.

Mark Band 1-Low Level
(1-2 marks)
The candidate demonstrates a basic knowledge of considerations with limited understanding shown; the material is basic and contains some inaccuracies. The candidate makes a limited attempt to apply acquired knowledge and understanding to the context provided.
The candidate provides nothing more than an unsupported assertion.
The information is basic and communicated in an unstructured way. The information is supported by limited evidence and the relationship to the evidence may not be clear.

0 marks
No attempt to answer the question or response is not worthy of credit

8
AO2 1a (4)
AO2 1b (4)

The following is indicative of possible factors/evidence that candidates may refer to but is not prescriptive or exhaustive:
Indicative Content:

<u>Inhabitants</u>
- Connection with the rest of the world
- Access to more information
- Up-to-date with news
- E-commerce
- Communication with people
- Can be used in schools/for education
- Cost (Devices and connection)

<u>Businesses</u>
- Sell products to wider audience//more customers
- Purchase items from wider range/more places
- Competitive prices
- Tourism can be advertised
- Online bookings for hotels

<u>Ethical issues</u>
- Access to inappropriate/illegal content
- Lead to social pressure to be online and get technology
- Cost
- Introduces digital and social divide
- Threats

<u>Privacy issues</u>
- Tracking of IPs/devices
- Social media
- Unwanted images and videos of people may be put online
- Risk of threats e.g. phishing/pharming/virus