

# **Cambridge Technicals IT**

## **Unit 2C: Essentials of cyber security**

Level 2 Cambridge Technical in IT  
**05883 - 05884**

## **Mark Scheme for June 2022**

OCR (Oxford Cambridge and RSA) is a leading UK awarding body, providing a wide range of qualifications to meet the needs of candidates of all ages and abilities. OCR qualifications include AS/A Levels, Diplomas, GCSEs, Cambridge Nationals, Cambridge Technicals, Functional Skills, Key Skills, Entry Level qualifications, NVQs and vocational qualifications in areas such as IT, business, languages, teaching/training, administration and secretarial skills.

It is also responsible for developing new specifications to meet national requirements and the needs of students and teachers. OCR is a not-for-profit organisation; any surplus made is invested back into the establishment to help towards the development of qualifications and support, which keep pace with the changing needs of today's society.

This mark scheme is published as an aid to teachers and students, to indicate the requirements of the examination. It shows the basis on which marks were awarded by examiners. It does not indicate the details of the discussions which took place at an examiners' meeting before marking commenced.

All examiners are instructed that alternative correct answers and unexpected approaches in candidates' scripts must be given marks that fairly reflect the relevant knowledge and skills demonstrated.

Mark schemes should be read in conjunction with the published question papers and the report on the examination.

© OCR 2022

## MARKING INSTRUCTIONS

### PREPARATION FOR MARKING

#### TRADITIONAL

Before the Standardisation meeting you must mark at least 10 scripts from several centres. For this preliminary marking you should use **pencil** and follow the **mark scheme**. Bring these **marked scripts** to the meeting.

#### MARKING

1. Mark strictly to the mark scheme.
2. Marks awarded must relate directly to the marking criteria.
3. The schedule of dates is very important. It is essential that you meet the traditional 40% Batch 1 and 100% Batch 2 deadlines. If you experience problems, you must contact your Team Leader (Supervisor) without delay.
4. If you are in any doubt about applying the mark scheme, consult your Team Leader by telephone or by email.
5. Work crossed out:
  - a. where a candidate crosses out an answer and provides an alternative response, the crossed out response is not marked and gains no marks
  - . if a candidate crosses out an answer to a whole question and makes no second attempt, and if the inclusion of the answer does not cause a rubric infringement, the assessor should attempt to mark the crossed out answer and award marks appropriately.
6. Always check the pages (and additional lined pages if present) at the end of the response in case any answers have been continued there. If the candidate has continued an answer there then add an annotation to confirm that the work has been seen.
7. There is a NR (No Response) option. Award NR (No Response)
  - if there is nothing written at all in the answer space
  - OR if there is a comment which does not in anyway relate to the question (e.g. 'can't do', 'don't know')
  - OR if there is a mark (e.g. a dash, a question mark) which isn't an attempt at the questionNote: Award 0 marks - for an attempt that earns no credit (including copying out the question)
8. Assistant Examiners will email a brief report on the performance of candidates to your Team Leader (Supervisor) by the end of the marking period. Your report should contain notes on particular strength displayed as well as common errors or weaknesses. Constructive criticism of the question paper/mark scheme is also appreciated.

Question		Answer	Marks	Guidance
1	(a)	<ul style="list-style-type: none"> <li>(Cyber) terrorists (1)</li> </ul>	1 (LO1.5)	Correct Answer Only (CAO)
	(b)	<ul style="list-style-type: none"> <li>Data Manipulation (1)</li> <li>Data Theft (1)</li> <li>Data Destruction (1)</li> </ul>	2 (LO1.4)	NOT data modification
	(c)	<ul style="list-style-type: none"> <li>Individuals (1)</li> <li>Equipment (by example) (1)</li> <li>Organisation (1)</li> </ul>	2 (LO1.3)	Two from list. DNA data / information as these are given in Q
2	(a)	<ul style="list-style-type: none"> <li>Taking a copy of the data (1) at a given point / time in the day (1)</li> <li>Storing the copy in a secure location / off site (allow an example) (1)</li> <li>Password protecting / encrypting the data (1)</li> <li>Any other valid suggestion</li> </ul>	3 (LO3.1)	
	(b)	<ul style="list-style-type: none"> <li>Users are aware (1) of the rules of using the (social media) website (1)</li> <li>AUP provides guidelines (1) of what can / cannot be posted / shared / commented (1)</li> <li>In case of a dispute (1) the AUP can be referred to (1)</li> <li>By signing the AUP (1) users are agreeing (1) to the rules (1)</li> <li>Any other valid suggestion</li> </ul>	3 (LO3.3.1)	

Question		Answer	Marks	Guidance
	(c)	<ul style="list-style-type: none"> <li>• Unauthorised access/hacking (1<sup>st</sup>)</li> <li>• A correct (1) username AND password must be entered to access the account (1)</li> <li>• Incorrect (1) user name and password will deny access to the account (1)</li> <li>• If incorrect user name and password (1) are entered multiple times / example then the account will be locked (1)</li> <li>• Any other valid suggestion</li> </ul>	3 (LO2.1)	<p>1<sup>st</sup> mark for identification 2<sup>nd</sup> &amp; 3<sup>rd</sup> marks for description</p> <p>To be considered for the description marks, the 1<sup>st</sup> mark must have been awarded.</p> <p>Read the WHOLE response as identification may not have been given in the type box.</p> <p>Allow data theft</p>
	(d)	<ul style="list-style-type: none"> <li>• Someone else/third party/hacker (1)</li> <li>• Gain access to personal details/accounts (by example) (1)</li> <li>• Pretending to be you/impersonate (1)</li> <li>• Details used without permission (1)</li> <li>• To obtain loans / goods / fraud / example (1)</li> <li>• Any other valid suggestion</li> </ul>	3 (LO2.1)	

Question		Answer	Marks	Guidance
	(e)	<ul style="list-style-type: none"> <li>• Access rights/permissions (1<sup>st</sup>) based on user names (1) which limit accessibility to data / information / device (1)</li> <li>• Biometric (1<sup>st</sup>) based on physical characteristic (1) example (1)</li> <li>• Anti-virus software (1<sup>st</sup>) checks for any viruses (1) and alerts user / automatically quarantines them (1)</li> <li>• Firewalls (1<sup>st</sup>) monitors traffic into and out of the network / device (when connected to the Internet) (1) and if traffic doesn't meet the rules it is denied access (1)</li> <li>• 2FA (1<sup>st</sup>) uses another device/app/email (1) to generate an OTP/Code/ confirm identity (1)</li> <li>• Any other valid suggestion</li> </ul>	6 (LO3.1)	<p>2 from list:</p> <p>1<sup>st</sup> mark for identification 2<sup>nd</sup> &amp; 3<sup>rd</sup> marks for description</p> <p>To be considered for the description marks, the 1<sup>st</sup> mark must have been awarded.</p> <p>The focus of the Q is <b>logical</b> methods</p> <p>The method must be appropriate for a portable device.</p>
3	(a)	<ul style="list-style-type: none"> <li>• To protect information / data (1)</li> <li>• To keep information / data confidential (1)</li> <li>• To maintain the availability of information / data (1)</li> </ul>	2 (LO1.2)	<p>2 from list</p> <p>DNA maintain the integrity of information &amp; data as this is given in the Q</p>
3	(b)	<ul style="list-style-type: none"> <li>• Customer details are stored on the laptop (1) and protecting these is a legislative requirement / example of legislation (1) to prevent hacking/information being released (1)</li> <li>• Business data / information is held on the laptop (1) and needs to be protected (1)</li> <li>• To ensure the florists stays safe (1) whilst online (1)</li> <li>• Any other valid suggestion</li> </ul>	2 (LO1.2)	

Question		Answer	Marks	Guidance	
3	(c)	<p><b>Financial (1)</b></p> <ul style="list-style-type: none"> <li>• May need to pay customers / suppliers' compensation (1) if details are stolen (1)</li> <li>• Any other valid suggestion</li> </ul> <p><b>Data (1)</b></p> <ul style="list-style-type: none"> <li>• Customer / supplier / stock data is held (1) may be difficult to get records back (1)</li> <li>• Any other valid suggestion</li> </ul> <p><b>Reputation (1)</b></p> <ul style="list-style-type: none"> <li>• Customers / suppliers may not want to deal with florist (1) if they know that details have been stolen (1)</li> <li>• Any other valid suggestion</li> </ul>	2 (LO2.4)	<p>Up to 2 marks available for a description of a loss impact</p> <p>It is possible to award marks without loss impact being specifically defined.</p>	
3	(d)	(i)	<ul style="list-style-type: none"> <li>• Computer Misuse Act (1)</li> </ul>	1 LO1.6)	<p>CAO Accept CMA/Computer Misuse, ignore any reference to date</p>
3	(d)	(ii)	<ul style="list-style-type: none"> <li>• The customer did not have authorisation to access the laptop / files stored on it (1) The Act makes it illegal (1) to carry out an unauthorised access (1)</li> <li>• Data stored on the laptop (1) has been deleted (1) which means that part 3 (of the CMA) has been broken. (1)</li> <li>• Example (1) e.g. Customer records have been deleted / the laptop has been accessed illegally</li> </ul>	4 (LO1.6)	<p>Up to 3 marks for an explanation, 1 mark available for an appropriate example.</p> <p>To be considered for marks for explanation mark for part (i) must have been awarded</p>
	(e)		<ul style="list-style-type: none"> <li>• Hacking (1) into the wi-fi as there is no security on the connection (1)</li> <li>• DOS/(DDOS) attack (1) flooding/overload the wireless point with data / making it inaccessible (1)</li> <li>• Theft (1) stealing the wifi access point (1)</li> <li>• Any other valid suggestion</li> </ul>	2 (LO2.2)	

Question	Answer	Marks	Guidance
(f)	<p>Indicative content</p> <p><b>Malware</b></p> <ul style="list-style-type: none"> <li>Any program or file that is harmful to a computer user.</li> <li>Types of malware can include computer viruses, worms, Trojan horses and spyware</li> </ul> <p><b>DoS</b></p> <ul style="list-style-type: none"> <li>A Denial of Service attack</li> <li>An attack where the attacker attempts to make a machine or network resource unavailable to its users by disrupting services of a host connected to the Internet.</li> <li>The attack floods the targeted machine or website with requests to attempt to overload systems and prevent legitimate requests from being fulfilled.</li> </ul> <p><b>Botnet</b></p> <ul style="list-style-type: none"> <li>A number of Internet-connected devices, each of which is running one or more bots.</li> <li>Can be used to carry out a distributed denial-of-service attack (DDoS attack),</li> <li>Can be used to steal data and send spam</li> <li>They allow the attacker to access a device and its connection.</li> </ul>	9 (LO2.3)	<p>Levels of response marking approach</p> <p><b>7-9 marks</b> Learner has shown a detailed level of understanding by discussing more than one system vulnerability that could lead to a cyber security attack on the florists. Relevant and appropriate examples are provided. Specialist terms will be used correctly and appropriately.</p> <p><b>4-6 marks</b> Learner has shown a good level of understanding by explaining at least one system vulnerability that could lead to a cyber security attack on the florists. Explanations may be limited in depth in the expansion(s). Some relevant examples are provided although these may not always be appropriate. Specialist terms will be used appropriately and for the most part correctly.</p> <p><b>1-3 marks</b> Learner has identified points relevant to system vulnerabilities that could lead to a cyber security attack on the florists. This may take the form of a bulleted list. Examples, if used, may lack relevance. There will be little, if any, use of specialist terms.</p> <p><b>0 marks</b> Nothing worthy of credit.</p> <p><i>These are the system vulnerabilities defined in the Spec</i></p>



**OCR (Oxford Cambridge and RSA Examinations)**  
**The Triangle Building**  
**Shaftesbury Road**  
**Cambridge**  
**CB2 8EA**

**OCR Customer Contact Centre**

**Education and Learning**

Telephone: 01223 553998

Facsimile: 01223 552627

Email: [general.qualifications@ocr.org.uk](mailto:general.qualifications@ocr.org.uk)

[www.ocr.org.uk](http://www.ocr.org.uk)

For staff training purposes and as part of our quality assurance programme your call may be recorded or monitored

**Oxford Cambridge and RSA Examinations**  
is a Company Limited by Guarantee  
Registered in England  
Registered Office; The Triangle Building, Shaftesbury Road, Cambridge, CB2 8EA  
Registered Company Number: 3484466  
OCR is an exempt Charity

**OCR (Oxford Cambridge and RSA Examinations)**  
Head office  
Telephone: 01223 552552  
Facsimile: 01223 552553

© OCR 2022

