Cambridge Technicals

IT

Unit 2C: Essentials of cyber security

Level 2 Cambridge Technical in IT
05883 - 05884

Mark Scheme for June 2024

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.

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
    b. 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 question
    Note: 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)**		• To maintain the integrity (of information and data) (1) • To maintain the availability (of information and data) (1)	2 LO1.2.1	Two from list These are taken from the unit specification
	(b)		• Data (1) • Information (1)	1 LO1.3.2	One from list These are taken from the unit specification
	(c)		• Cyber criminals • Cyber terrorists • Hackers • Phishers	2 LO1.5.1	Two from list These are taken from the unit specification
2	**(a)**		• DPA / GDPR (1)	1 LO1.6.1	Correct Answer only (CAO)
	(b)		• Access to a device / data / information (1) without permission (1) • Any other valid suggestion	2 LO2.1.6	

	(c)		• Hacker (1st)
			 • (Uses a device to maliciously) access another device/account (1) to:
			   ○ steal / manipulate / data (1)
			   ○ install a virus (1)
			   ○ example (1)
			 • Any other valid suggestion
				3
				 LO1.5.1c
					1st mark for identification
					 2nd / 3rd marks for description
					
					 If type of attacker is not clear in the first box, continue reading and award in description.

Question			Answer	Marks	Guidance
(d)			• Disables/covers/blocks USB ports (1) • Requires a key to unlock (1) • Any other valid suggestion	1 LO3.2.6b	
(e)			• To protect the laptop/data on the laptop (1) from unauthorised external storage media (1) • Any other valid suggestion	2 LO3.2	Up to 2 marks for a complete description of the purpose of a device lock

(f)			• Financial (1st)
			    ○ clients moving (1) to a different driving instructor (1)
			    ○ access to bank account details (1) steal money (1)
			• Data (1st)
			    ○ stored on the laptop may have been stolen (1) meaning time taken to restore the data (1)
			• Reputation (1st)
			    ○ client details could be stolen (1) which could lead to clients not trusting the driving instructor (1)
				6
				LO2.4.1
					For each of 2 loss impacts:
					• 1st mark for identification
					• 2nd / 3rd marks for description
					
					These are the loss impacts taken from the unit specification.
					
					Question does not specify if to the driving instructor or to the clients – allow both
					
					Allow mix and match if relevant
					
					DNA intellectual property as this is given in the question

Question			Answer	Marks	Guidance

3	**(a)**		• Adware (1st)
			    o software that automatically (1) downloads advertisements / pop-ups / banners (1)
			• Spyware (1st)
			    o software installed without the user's knowledge (1) to gather information (1)
			• Clickjacking (1st)
			    o a user clicks on a webpage component (1) which is invisible / disguised as a different component (1)
			• Virus (1)
			    o spreads between computers (1) and causes damage to data/software (1)
			• Worm (1)
			    o self-replicate from one computer to another (1) without human activation (1)
			• Any other valid suggestion
				6
				 LO2.1.4
					For each of 2 malware:
					• 1st mark for identification
					• 2nd / 3rd marks for description

	(b)		• Equipment (1)	1 LO1.3.3	CAO
	(c)		• Useless traffic/pings (1) will be sent to a webpage / site (1) so customers of the travel agent cannot login / access the webpage/site (1) • Any other valid suggestion	3 LO 2.2.1	

Question			Answer	Marks	Guidance
	(d)		• Financial gain (1) • Publicity (1) • Fraud (1) • Espionage (1) • Thrill seeking / entertainment (1)	2 LO1.5.2	1 mark for each of 2 motivations identified These are taken from the unit specification
	(e)		• Computer Misuse Act / CMA (1)	1 LO1.6.2	CAO Ignore any reference to date or lack of
	(f)		• Personal / contact details (1) of clients will be stored (1) • Client payment details may be stored (1) • Data / information (1) needs to be protected (1) • Legal requirements (1) to comply with DPA (1) • Improve reputation (1) so customers trust it (1) and return (1) Any other valid suggestion	3 LO1.2.2	Up to 3 marks for a complete explanation of why it is important that the travel agent increases their cyber security

Question			Answer	Marks	Guidance

	(g)		**Indicative content**
			
			• Having a password policy can help reduce chances of a cyber security incident
			• To provide guidelines to staff at the travel agents
			• Defines the rules relating to:
			   ○ The format of passwords
			   ○ How often they should be changed
			   ○ Usage of the same password
			• Provides guidance relating to strong / weak passwords
			• Guidance on the use of passwords / phrases
			• Defines best practices relating to passwords
			• Sets out procedures in case of a security breach relating to passwords.
				9
				LO3.3.6
					Levels of response marking approach
					
					7-9 marks
					Learner has shown a detailed level of understanding by explaining the importance of a password policy. Relevant and appropriate examples are provided. Specialist terms will be used correctly and appropriately.
					
					4-6 marks
					Learner has shown a good level of understanding by describing the importance of a password policy. Descriptions 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.
					
					1-3 marks
					Learner has identified points relevant to a password policy
					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.
					
					0 marks
					Nothing worthy of credit.

Need to get in touch?

If you ever have any questions about OCR qualifications or services (including administration, logistics and teaching) please feel free to get in touch with our customer support centre.

Call us on

01223 553998

Alternatively, you can email us on

support@ocr.org.uk

For more information visit

ocr.org.uk/qualifications/resource-finder

ocr.org.uk

Twitter/ocrexams

/ocrexams

/company/ocr

/ocrexams