OCR
Oxford Cambridge and RSA

Cambridge Technicals
IT

Unit 2: Essentials of cyber security

Level 2 Cambridge Technical in IT
05883 - 05884

Mark Scheme for January 2020

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 2020

Question			Answer	Marks	Guidance
1	(a)		• Data destruction (1) • Data modification (1) • Data theft (1) • Denial of service (1) • Phishing (1) • Pharming (1)	2 (LO1.4)	Two from list
	(b)		• Individuals (1) • Data (1) • Information (1) • Equipment (1) • System (1)	2 (LO1.3)	Two from list
	(c)		• To protect information/data (1) • To keep information/data confidential (1) • To protect system from infection (1) • To maintain the availability of information/data (1) • To protect identity/prevent identity theft (1)	1 (LO1.2)	One from list
2	(a)	(i)	• Fraudulent websites (1) • Fraudulent webpage (1) • Pharming (1) • Any other valid suggestion	1 (LO2.1)	One from list
	(a)	(ii)	• Customers clicking (1) on a rogue hyperlink (1) on the website (1) • Customer is redirected (1) from the genuine/real site (1) to a fake site (1) • Any other valid suggestion	3 (LO2.2)	

Question			Answer	Marks	Guidance
	(a)	(iii)	• Identity theft (1st) customer details could be stolen (1) when inputting details on the fraudulent booking webpage (1) • Virus (1st) the fraudulent booking webpage may download (1) a virus when customers input details / submit the booking request (1) • Hoax emails (1st) when customer input their email address (1) this could be used by the cyber attackers (1) • Denial of service (1) disruption to the service (1) by overloading the server with requests (1) • Any other valid suggestion	3 (LO2.1)	The type of threat must be correct to enable marks for the description to be awarded.
	(b)		• Scammer (1st) • A person who attempts to steal money (1) by deception/ tricking the victim (1) • Phisher (1st) • Poses an employee (1) to get customer to give up details/sends fake emails (1) • Any other valid suggestion	3 (LO1.5)	The type of cyber attacker must be correct to enable marks for the description to be awarded.
	(c)		• Data/information (1st) customer records / financial / film history (1) held by the cinema (1) • Equipment (1st) storage devices (1) used to hold records / run the website (1) • Any other valid suggestion	3 (LO1.3)	The target must be correct to enable marks for the description to be awarded. Allow responses based on specific types of organisations such as government organisations, health service etc.

Question			Answer	Marks	Guidance
	(d)		• Scrambles / (1) the card number / start / end dates / CVO number(1) so that they are unreadable / not understandable (1) • these can only be unscrambled / decrypted (1) by using an encryption code (1) • If the card details are accessed (1) by someone without the encryption code (1) then they will be meaningless (1) • Any other valid suggestion	3 (LO3.)1	Allow alternative words for scrambles – encodes/codes
3	**(a)**		• Customer personal details are stored (1) • Customer payment details are stored (1) • To meet legislative requirements/GDPR/Data Protection (1) • To protect customer information/data (1) • To keep customer information/data confidential (1) • To maintain the integrity of customer information/data (1) • To prevent virus destroying/accessing customer data (1) • Any other valid suggestion	2 (LO1.2)	
	(b)		• Backup could be used to restore customer records (1) depending on when the backup was taken (1) little customer record data may be missing (1) • Backups may be securely stored (1) so may not have been affected by the attack. (1) meaning the data will not be lost (1) • Any other valid suggestion	3 (LO3.1)	

Question			Answer	Marks	Guidance
	(c)		• Access rights and permissions (1st) based on usernames (1) which limit accessibility to records (1) • (token) authentication (1st) when the username / password is input (1) a token / code is emailed to the account to be input before access is granted (1) • Anti-virus software (1st) checks for any viruses (1) and alerts user / automatically quarantines them (1) • Firewalls (1st) monitors traffic into and out of the cloud storage area (1) and if traffic doesn't meet the rules it is denied access (1) • Token authentication (1) additional layer of security (1) message sent to second device (1) • Any other valid suggestion	6 (LO3.1)	Two from list The type of protection must be correct to enable marks for the description to be awarded. 1st mark for the protection method, up to 2 for description Must be appropriate to securing the cloud-based customer records DNA Usernames / passwords, secure backups or encryption and token authentication
	(d)		• A program that replicates itself (1) so it can spread to other computer devices (1) • Deletes data (1) • Any other valid suggestion	2 (LO2.1)	
	(e)		• Financial gain (1) • Publicity (1) • Fraud (1) • Malicious intent (1) • Any other valid suggestion	2 (LO1.5)	Not espionage or political

Question			Answer	Marks	Guidance
	(f)		Indicative content **Supplier** • Customers' electricity readings may have been changed so bills are inaccurate • Payments may be delayed • Difficulty in identifying which records have been edited / deleted • Extra staff may be needed to investigate / solve the issues caused • Some payments may be made twice so supplier will need to refund the extra payment • The backup may not be fully up to date depending on the time difference between the backup being taken and the attack • Any other valid suggestion **Customers** • Incorrect bills may be issued meaning payments are wrong • Payments may be missed leading to issues with credit referencing • Payments made may not be on the customer records • Identity theft may occur as contact details may have been accessed • Bank details are stored so accounts may be accessed, and money stolen • Credit cards / loans may be taken out by the attackers with no knowledge of the customers Any other valid suggestion.	9 (LO2.4)	Levels of response marking approach **7-9 marks** Learner has shown a detailed level of understanding by discussing the disruption that may occur. The supplier **and** customers are considered 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 explaining the disruption that may occur. Explanations may be limited in depth in the expansion(s). The supplier and / or the customer are considered. 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 the disruption that may occur. 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.

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

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 2020