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 2021

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.

Question			Answer	Marks	Guidance
1	(a)		• Computers (1) • Programs (1) • Data (1) • Information (1) • Individuals / People / Employees / Customers (1)	2 (LO1.1)	Two from list Allow examples of data
	(b)		• (Data) theft (1) • Deletion (1) • Destruction (1)	1 (LO1.4)	One from list
	(c)		• Computer Misuse Act (1)	1 (LO1.6)	CAO
	(d)		• To maintain the integrity of information/data (1) • To maintain the availability of information/data (1) • To protect information/data (1)	1 (LO1.2)	One from list
2	(a)		• System (1)	1 (LO2.3)	CAO
	(b)		• The network will be flooded (1) with traffic (1) making it unavailable to users (1) server cannot handle traffic (1) • Any other valid suggestion	3 (LO2.1)	

Question			Answer	Marks	Guidance
	(c)		• Operational (1) Data may have been lost during the attack (1) it will take time to install any backups of data(1) • Operational (1) the backups may not include the most up-to-date data (1) so there may be a time delay to recover the latest data (1) • Commercial (1) the shops will not be able to fully carry out (1) the day-to-day running of the shops (1) • Financial (1) customers may not be able to place orders for ice cream (1) leading to loss of revenue (1) • Financial (1) increased costs may be incurred (1) as the shops have to improve the security (1) • Financial (1) customers cannot place orders (1) loss of reputation (1) • Any other valid suggestion	3 (LO2.4)	Max 2 if no identification of type of impact – impact can be inferred
	(d)		• A type of malware (1) that allows an attacker to take control of a system (1) without the users knowledge (1) • Group of computers (1) infected with malware (1) controlled by third party (1) • Any other valid suggestion	3 (LO2.1)	
	(e)		• Virus (1) • Trojan (1) • Ransomware (1) • Adware (1) • Spyware (1) • Any other valid suggestion	2 (LO2.1)	Two from list

Question			Answer	Marks	Guidance
	(f)		• Phisher (1st) • The emails pretend to be from the ice cream shops (1) • The link in the email (1) takes the supplier to a fake website (1) • To get them to enter personal information (1) into a fake website (1) • Any other valid suggestion	3 (LO1.5)	The type of attacker must be correct before marks for the description can be awarded.
3	**(a)**		• Customer personal / payment details are stored (1) • Customer personal / payment details must be kept secure (1) • Business data must be kept secure (1) • To meet legislative requirements (1) • Any other valid suggestion	2 (LO1.2)	Two from list
	(b)	**(i)**	• Hacker/Cyber criminal / cyber terrorist (1st) • (Hackers) find a weakness in a computer system (1) and exploits / gains unauthorised access (1) • Uses their technical knowledge (1) • Any other valid suggestion	3 (LO1.5)	The type of attacker must be correct before marks for the description can be awarded.
		(ii)	• Financial gain (1) • Publicity (1) • Fraud (1) • Espionage (1) • Revenge (1)	1 (LO1.5)	One from list

Question			Answer	Marks	Guidance
	(c)	(i)	• Virus/Malware (1st) o Files / films are infected (1) when the file / film is streamed the virus is included (1) • Insider (1st) o Employee from within the organisation (1) changed the file before it was uploaded (1) • Unauthorised access /hacker (1st) o Accessed the system (1) without authorisation (1) changed the contents of the file (1) • Any other valid suggestion	3 (LO2.1)	The type of threat must be correct before marks for the description can be awarded.
		(ii)	• Anti-virus software (1st) o Tries to detect a virus (1) before it enters the system (1) o If a virus is detected (1) it is removed / quarantined (1) • Passwords (1st) o Required before access is granted (1) combination of letters and numbers (1) can be biometric (1) • Any other valid suggestion	3 (LO3.1)	The protection method must be correct before marks for the description can be awarded.
		(iii)	• By clicking a link (1) in an email (1) which downloads a virus to the files / films / TV programmes (1) • Downloading files (1) from a website (1) which includes a virus which is installed when the file is saved (1) • Employee overlooked for promotion (1) not monitored (1) and takes revenge (1) • Any other valid suggestion	3 (LO2.2)	This how the threat occurred, not an accidental way of how the video was corrupted / uploaded.

Question			Answer	Marks	Guidance
	(d)		• Data destruction/erasure (1) • Data modification (1)	1 (LO1.4)	
	(e)		Indicative content • CoC sets out what is and is not acceptable behaviour • Sets down policy and procedures relating to the operation of the customer relations team and how customer data should be processed / accessed. • All team members will have access to the CoC • May have to sign that they have read and understood the contents • This agreement can be used in case of any breach by a team member • Defines how customer data can be collected / used • Explains the security procedures that have to be carried out when dealing with customers e.g. asking security questions • Defines how customer data should be processed and stored Any other valid suggestions	9 (LO2.4)	Levels of response marking approach **7-9 marks** Learner has shown a detailed level of understanding by discussing how a CoC will increase security. 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 how a CoC will increase security. 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 the use of a CoC to increase security. 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