Cambridge Technicals
IT

Unit 2: Essentials of cyber security

Level 2 Cambridge Technical in IT
05883 - 05884

Mark Scheme for June 2019

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)		• Blagging (1) • Pharming (1) • Phishing (1) • Shouldering (1) • Hacking (1) • Scamming (1)	2 (LO2.1)	Points marking Two from list
	(b)		• Data modification (1)	1 (LO1.4)	Correct Answer Only (CAO)
	(c)		• Financial (1) • Fraud (1) • Espionage (1)	2 (LO1.5)	Points marking approach
2	(a)		• Fake / hoax emails (1) • Phishing/scamming (1st) • Sending emails pretending to be from the organisation (1) to get information (1)	4 (LO2.1)	CAO The type of attack must be correct to enable marks for the description to be awarded. 1st mark for attacker, up to 3 for description There aren't any other valid suggestions.
	(b)		• Data Protection Act / DPA (1)	1 (LO1.6)	CAO
	(c)		• Identity Theft (1) personal details are stolen (1) and used for financial gain by another person / example (1) • Goods being ordered (1) without the customer's knowledge (1) with payment being taken from their debit / credit card (1) • Any other valid suggestion	6 (LO2.4)	Points marking Two from list

Question			Answer	Marks	Guidance
	(d)		• Requires access details / user name & password (1) • (when entered) a code is provided for entry by user (1) • Any other valid suggestion	2 (LO3.1)	Points marking approach
	(e)		• A policy that sets down/states (1) who can use / access files and folders (on a network) (1) • Defines what (access) rights (1) a user has to files and folders (1) • Example (1) e.g. restricting access to files and folders containing customer data • Any other valid suggestion	3 (LO3.3)	Points marking approach To be awarded full marks an example must be provided
3	**(a)**		• Malware (1st) installed on a device (1) and collects information about users (1) • DoS (1st) Floods a device with traffic (1) to make it stop functioning (1) • Botnet (1st) takes control of a device (1) without the users knowledge (1) • Any other valid suggestion	3 (LO2.3)	The type of vulnerability must be correct to enable marks for the description to be awarded. 1st mark for vulnerability, up to 2 for description
	(b)		• Hacking (1st) a weakness is found (1) and exploited (1) • Clicking on a hyperlink (1st) usually in an email (1) the link takes the user to a false website (1) • Any other valid suggestion	3 (LO2.2)	The type of threat must be correct to enable marks for the description to be awarded. 1st mark for threat, up to 2 for description

Question			Answer	Marks	Guidance
	(c)		• Adware (1) • Spyware (1) • Clickjacking (1) • Trojan Horse (1) • Virus (1) • Worm (1) • Any other valid suggestion	2 (LO2.1)	Points marking 2 from list
	(d)		• Monitors (1) incoming traffic (1) and outgoing traffic (1) • Decides (1) if the traffic should be blocked or allowed (1) based on a set of rules (1) • Establishes a barrier (1) between the PDA and the internet (1) • Example (1) e.g. can block websites that do not meet the rules • Any other valid suggestion	4 (LO3.1)	Points marking approach To be awarded full marks an example must be provided
	(e)		• User name & password (1st) to enable internet access (1) a correct user name & password must be entered (1) • Authentication (1st) a process is put in place to verify (1) the authenticity / credentials of the user (1) • Any other valid suggestion	3 (LO3.1)	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 a home situation DNA Firewalls and token authentication

Question			Answer	Marks	Guidance
	(f)		Indicative content Purpose of cyber security. • To secure the PDA and internet access point from an attack • To protect data and information that can be accessed by the PDA • To protect the software that enables the PDA and internet access point to operate efficiently • Any other valid suggestion Importance • The PDA has access to personal information such as location and credit / debit cards. • The PDA can carry out functions in the house such as turning lights on and off • A cyber attacker / hacker can access the internet access point as no security procedure is in place to connect to it. • The unsecured internet access point could enable malware / virus etc. to be uploaded to affect the PDA • If the internet access in the house is limited then the cyber attacker could use up the internet access • Any other valid suggestion	9 (LO1.2)	Levels of response marking approach **7-9 marks** Learner has shown a detailed level of understanding by discussing the importance of cyber security. The PDA and internet access point are both 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 importance of cyber security. Explanations may be limited in depth in the expansion(s). The PDA and / or the internet access point 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 importance of cyber 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