Cambridge Technicals
IT

Unit 2C: Essentials of cyber security

Level 2 Cambridge Technical in IT
05883 - 05884

Mark Scheme for January 2023

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.

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 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)**		• Data destruction (1) • Data manipulation (1) • Data modification (1) • Phishing (1) • Pharming (1) • DoS (1)	1 (LO1.4)	One from list DNA Cyber Theft
	(b)		• Cyber terrorists (1) • Hackers (1) • Scammers (1) • Phishers (1)	2 (LO1.5)	Two from list DNA cyber criminals
	(c)		• To protect data / information (1) • To keep data / information confidential (1) • To maintain the integrity of the data / information (1) • Protect against malicious software (1)	2 (LO1.2)	Two from list. DNA maintain the availability of information / data
2	**(a)**	**(i)**	• A person who engages in criminal activity/breaks the law (1) by means of computers/ the Internet. (1) • Any other valid suggestion	2 (LO1.5)	Up to 2 marks for definition of a cybercriminal DNA example of cyber criminal
	(a)	**(ii)**	• Financial gain (1) • Publicity (1) • Fraud (1)	2 (LO1.5)	Two from list DNA Espionage
	(a)	**(iii)**	• DPA (1) • GDPR (1) • Computer Misuse Act (1)	1 (LO1.6)	For 1 mark, 1 from list The year is not required

Question			Answer	Marks	Guidance
	(b)	**(i)**	- Virus (1st) a piece of code (1) which has a negative effect on a computer system (1) - Malware (1st) software that is specifically designed (1) to disrupt / change a computer system (1) - Website content changed (1st) original images edited/deleted (1) new ones containing adverts uploaded (1) - Any other valid suggestion	6 (LO2.1)	2 from list: 1st mark for identification 2nd & 3rd marks for description To be considered for the description marks, the 1st mark must have been awarded.
	(b)	**(ii)**	- DoS (1st) Floods a device with traffic (1) to make it stop functioning (1) - Any other valid suggestion	3 (LO2.2)	1st mark for identification 2nd & 3rd marks for description To be considered for the description marks, the 1st mark must have been awarded.
2	**(c)**	**(i)**	- To check/scan for any viruses (1) and alert user / automatically quarantines them (1) removes them (1) - Any other valid suggestion	2 (LO3.1)	Up to 2 marks for a description of the purpose of anti-virus software
	(c)	**(ii)**	- Real time (1) updating (1) - Automatic (1) updates (1) - Library (1) of virus signatures (1) - Permanently (1) scanning (1) - User (1) can force a scan (1) - Schedule (1) regular scans (1) - Any other valid suggestion	2 (LO3.1)	Up to 2 marks for a description of a characteristic of anti-virus software

	Question		Answer	Marks	Guidance
3	**(a)**		• To protect (1) the personal data (1) of the gamers/children/parents (1) • To protect (1) the games (1) data / code (1) • Children's data is stored (1) specific responsibility (1) to keep safe (1) • To prevent a hacker (1) gaining access to personal details (1) and payment information (1) • Legal requirement (1) DPA (1) requires security (1) • Any other valid suggestion	3 (LO1.2)	Up to 3 marks for an explanation of why cyber security is important
	(b)		• 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 games data (1) and the internet (1) • Blocks data (1) from IPs (1) on black list/locations (1) • Filters (1) based on ruleset (1) • Any other valid suggestion	3 (LO3.1)	Up to 3 marks for an explanation of how a firewall will protect the games data stored on the server.
	(c)		• Scans are taken of characteristics / example (1) and stored as digitised records (1) these are matched to the records of authorised users (1) a match enables access (1) • Max 1 for example of RFID e.g. fingerprint, face (1) • Any other valid suggestion	3 (LO3.2)	Up to 3 marks for how a biometric access device can be used to protect the server room

Question			Answer	Marks	Guidance
	(d)		• Mixture of upper/lower-case/number/symbol (2 out of 3 required) (1) • Special characters (Accept examples) (1) • Minimum length (accept any number 8 or more) (1) • No memorable words (accept example such as name of children) (1) • Non dictionary word (1) • Three word phrase (1) • A different password to any others/previous ones used (1) • Any other valid suggestion	1 (LO3.3)	1 mark for an identification of a password rule
	(e)		• Phishing/Phisher (1st) • The emails pretend to be from the games company (1) • The link in the email takes the parent to a fake website (1) • Any other valid suggestion	3 (LO1.5)	

Question		Answer	Marks	Guidance
	(f)	**Indicative content** • Code may get into the public domain • Other companies may use the code and provide the games cheaper as there is no development cost • Reduction in number of customers leading to loss of revenue • Job losses as customers move to different companies • Other companies may copy the games or characters	9 (LO2.4)	Levels of response marking approach **7-9 marks** Learner has shown a detailed level of understanding by explaining more than one impact of the loss of intellectual property following a cyber-attack. 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 at least one impact of the loss of intellectual property following a cyber-attack. 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 impact of the loss of intellectual property following a cyber-attack. 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