

**Cambridge Technicals  
IT**

**Unit 3: Cyber Security**

Level 3 Cambridge Technical in IT  
**05838 – 05842/05877**

**Mark Scheme for January 2022**

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 2022

Abbreviations, annotations and conventions used in the detailed Mark Scheme (to include abbreviations and subject-specific conventions).

Annotation	Meaning
/	alternative and acceptable answers for the same marking point
✓	Separates marking points
<b>DO NOT ALLOW</b>	Answers which are not worthy of credit
<b>IGNORE</b>	Statements which are irrelevant
<b>ALLOW</b>	Answers that can be accepted
( )	Words which are not essential to gain credit
—	Underlined words must be present in answer to score a mark
<b>ECF</b>	Error carried forward
<b>AW</b>	Alternative wording
<b>ORA</b>	Or reverse argument

**Subject-specific Marking Instructions****INTRODUCTION**

Your first task as an Examiner is to become thoroughly familiar with the material on which the examination depends. This material includes:

- the specification, especially the assessment objectives
- the question paper
- the mark scheme.

You should ensure that you have copies of these materials.

You should ensure also that you are familiar with the administrative procedures related to the marking process. These are set out in the OCR booklet **Instructions for Examiners**. If you are examining for the first time, please read carefully **Appendix 5 Introduction to Script Marking: Notes for New Examiners**.

Please ask for help or guidance whenever you need it. Your first point of contact is your Team Leader.

Question			Answer	Marks	Guidance
1	(a)	(i)	<p>2 marks each, 2 from e.g: OS Updates</p> <ul style="list-style-type: none"> <li>• Patch/fix any mistakes in the code (1)</li> <li>• Prevent known vulnerabilities being used (1)</li> </ul> <p>Anti-malware</p> <ul style="list-style-type: none"> <li>• Find any malware on the device/makes sure there is no malware on the device (1)</li> <li>• Removes malware from device (1)</li> <li>• Prevents malware getting on the device (1)</li> </ul>	4	<p>Accept virus for malware</p> <p>OS Updates – their answers need to be about protecting the data NOT improving the software/adding features</p>
	(a)	(ii)	<p>3 marks each, 1 for identification, 2 for description e.g:</p> <ul style="list-style-type: none"> <li>• Biometric (1) use of fingerprint/face (1) to only allow access/unique to one individual (1)</li> <li>• Passcodes/password/patterns (1) use of specific sequence of numbers/letters/pattern (1) only allow access to individuals that know the code (1) (1)</li> <li>• Encryption (1) turning the data into meaningless text (1) until the key is applied (1)</li> <li>• Removeable media/cloud (1) storing the data on an external device (1) which can be removed from the device (1)</li> <li>• Two-factor authentication (1) access to a second device/ email to access data needed (1)</li> <li>• Firewall (1) acts as a barrier between the phone and the network (1) and filters incoming and outgoing traffic.</li> <li>• Privacy screens (1) to prevent shoulder surfing (1)</li> <li>• Avoid insecure networks (1) do not connect to unknown wifi networks (1) or networks without authentication (1)</li> </ul>	6	<p>NOT os updates or anti-malware/anti virus</p> <p>If no identification, 0 marks</p> <p>Must be appropriate for a phone</p>

Question		Answer	Marks	Guidance
	(b) (i)	<p>2 marks each, 2 from:</p> <ul style="list-style-type: none"> <li>• Account Lockout: <ul style="list-style-type: none"> <li>○ Shut them out of the account/cannot access the account (1)</li> <li>○ Hacker changes login details (1)</li> <li>○ Cannot use existing password/username to get into account / changed credentials(1)</li> <li>○ Can be a time period before reattempt of password allowed /access (1)</li> <li>○ Multiple login attempts leads to automatic lockout (1)</li> </ul> </li> <li>• Destruction <ul style="list-style-type: none"> <li>○ Data no longer accessible/been removed/wiped/deleted (1)</li> <li>○ E.g. Remove membership information (1)</li> </ul> </li> </ul>	4	
	(b) (ii)	<p>1 from:</p> <ul style="list-style-type: none"> <li>• Hacking (1)</li> <li>• Escalation of privileges (1)</li> <li>• Information disclosure (1)</li> <li>• Modification of data (1)</li> <li>• Denial of service (1)</li> <li>• Theft / Identity theft (1)</li> </ul>	1	NOT account lockout or destruction

Question	Answer	Marks	Guidance
(c)	<p>2 marks each, 2 from e.g:</p> <ul style="list-style-type: none"> <li>• Accidental <ul style="list-style-type: none"> <li>○ Not malicious/intended/unintentional (1) there is no motive behind the threat (1)</li> <li>○ As a result of negligence (1) leaving the phone unlocked (1)</li> <li>○ Lack of education (1) not knowing how to set a passcode (1)</li> <li>○ Inattention to surroundings (1) someone shoulder surfing them (1)</li> <li>○ Reusing passwords (1) so if one account is hacked they all are (1)</li> </ul> </li> <li>• Intentional <ul style="list-style-type: none"> <li>○ Targeted attack (1) result of direct action (1)</li> <li>○ Sending links (1) that infect the phone when clicked (1)</li> <li>○ Cancelling updates (1) so vulnerabilities still exist (1)</li> <li>○ Malicious reason (1)</li> </ul> </li> </ul>	4	Allow specific +examples
(d)	<p>2 from, 2 marks each e.g:</p> <ul style="list-style-type: none"> <li>• Shoulder surfing (1) watching someone enter their passcode (1)</li> <li>• Brute force (1) attempting multiple passwords (1)</li> <li>• Virus/spyware/keylogger/malware (1) e.g (spyware) watching E James enter the passwords / (Keylogger) recording keystrokes to find the password (1)</li> <li>• Man The Middle (1) collecting usernames and passwords when transmitted (1)</li> <li>• Phishing (1) gain details from emails (1)</li> </ul>	4	<p>Must be appropriate for a phone Social Engineering is TV</p> <p>Second mark for keylogger/spyware etc must relate to the type of malware for the mark</p>

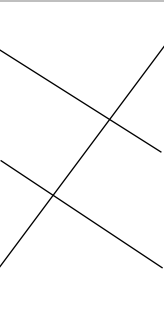
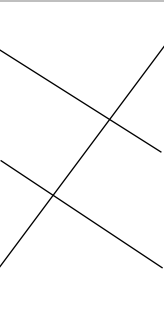
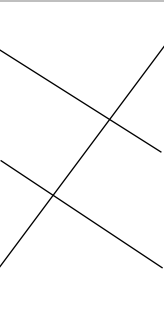
Question		Answer	Marks	Guidance
	(e) (i)	2 from e.g: <ul style="list-style-type: none"> <li>• Change passwords (1) on all accounts/before used (1)</li> <li>• Notify company to freeze accounts (1) so they cannot get access (1)</li> <li>• Add 2FA (1) so more than password is required (1)</li> </ul>	2	
	(e) (ii)	3 from e.g: <ul style="list-style-type: none"> <li>• If password is changed the one stolen (1) will be useless (1) access to the account cannot be gained (1)</li> <li>• If accounts are frozen no one can gain access (1) so data cannot be obtained (1) and knowing the password is pointless (1)</li> <li>• Two items are required for 2FA (1) so just the password is not enough (1) as cannot gain access (1)</li> </ul>	3	Action must continue from the one described in e(i)
	(e) (iii)	1 from e.g: <ul style="list-style-type: none"> <li>• Change passwords (1)</li> <li>• Notify company to freeze accounts (1)</li> <li>• Add 2FA (1)</li> </ul>	1	Must be different from e(i)



Question	Answer	Marks	Guidance								
2	<p>Indicative content may include:</p> <p>The issues surrounding having all the passwords stored in one place</p> <ul style="list-style-type: none"> <li>• If the manager is hacked then all passwords will be released</li> <li>• If the master password to the password manager is lost then cannot gain access to any accounts.</li> </ul> <p>The issues surrounding complex passwords</p> <ul style="list-style-type: none"> <li>• User does not have to come up with complicated passwords as the password manager will do this</li> <li>• User does not have to remember complicated passwords as the manager stores them all</li> <li>• Only need to remember one password – for the manager not lots of other ones.</li> </ul> <p>The issues surrounding ethical business practices</p> <ul style="list-style-type: none"> <li>• Does the company comply with the legal requirements? Of its country and the country where the password manager is being used</li> <li>• Is the data stored in a secure way to prevent insider threats – such as encrypted data, restricted access</li> <li>• Web server backup and availability – if it does not work then the user cannot get access to their passwords</li> </ul> <p>Other issues</p> <ul style="list-style-type: none"> <li>• When the user transfers phones, the passwords can all be transferred through the app – does not have to reinput them and make mistakes</li> </ul>	10	<p>Level of response marking:</p> <table border="1" data-bbox="1384 323 2069 1378"> <tbody> <tr> <td data-bbox="1384 323 1496 762">7 - 10 marks</td> <td data-bbox="1496 323 2069 762"> <p>Candidate has evaluated the use of a password manager. Both positive AND negative benefits of the use of a password manager have been analysed and the candidate is able to make informed and appropriate judgements within the context provided. An implied conclusion is present which is informed by the supporting analysis.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p> </td> </tr> <tr> <td data-bbox="1384 762 1496 1070">4 – 6 marks</td> <td data-bbox="1496 762 2069 1070"> <p>Candidate has described the use of a password manager. Positive OR negative benefits of the use of a password manager have been described and the candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p> </td> </tr> <tr> <td data-bbox="1384 1070 1496 1310">1 – 3 marks</td> <td data-bbox="1496 1070 2069 1310"> <p>Candidate has identified benefits (positive OR negative) of using a password manager.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p> </td> </tr> <tr> <td data-bbox="1384 1310 1496 1378">0 marks</td> <td data-bbox="1496 1310 2069 1378">Nothing worthy of credit.</td> </tr> </tbody> </table>	7 - 10 marks	<p>Candidate has evaluated the use of a password manager. Both positive AND negative benefits of the use of a password manager have been analysed and the candidate is able to make informed and appropriate judgements within the context provided. An implied conclusion is present which is informed by the supporting analysis.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>	4 – 6 marks	<p>Candidate has described the use of a password manager. Positive OR negative benefits of the use of a password manager have been described and the candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p>	1 – 3 marks	<p>Candidate has identified benefits (positive OR negative) of using a password manager.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p>	0 marks	Nothing worthy of credit.
7 - 10 marks	<p>Candidate has evaluated the use of a password manager. Both positive AND negative benefits of the use of a password manager have been analysed and the candidate is able to make informed and appropriate judgements within the context provided. An implied conclusion is present which is informed by the supporting analysis.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>										
4 – 6 marks	<p>Candidate has described the use of a password manager. Positive OR negative benefits of the use of a password manager have been described and the candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p>										
1 – 3 marks	<p>Candidate has identified benefits (positive OR negative) of using a password manager.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point.</p>										
0 marks	Nothing worthy of credit.										

Question		Answer	Marks	Guidance
3	(a)	2 from e.g.: <ul style="list-style-type: none"> <li>• Recovery time (1)</li> <li>• Customer retention (1)</li> <li>• Customer loyalty (1)</li> <li>• Reputation (1)</li> <li>• Business (1)</li> <li>• Financial (1)</li> </ul>	2	Allow examples
	(b)	2 from, 2 marks each e.g: <ul style="list-style-type: none"> <li>• Technique/vulnerability used (1) and how to prevent it happening again (1)</li> <li>• Type of attacker (1) and how to target them in the future (1)</li> <li>• Review of procedures (1) were the steps taken correct (1)</li> <li>• Review of documentation (1) was it followed correctly (1)</li> <li>• Review of what/who was targeted(1) what damage was caused (1)</li> <li>• Review of PR (1) was it done correctly (1)</li> </ul>	4	

Question		Answer	Marks	Guidance	
(c)		<p>Indicative content may include:</p> <ul style="list-style-type: none"> <li>• Allow you to see what is happening in the network and create a baseline that you can judge any intrusions by.</li> <li>• Allow for algorithms and programs to be run against the system to detect any changes</li> <li>• Allow for notifications of changes to be sent 24/7 that can be analysed by a human</li> <li>• They can work in real time giving an up-to-date state of network</li> <li>• Does not make any changes or stop any intruders so based on how long it takes a human to react the damage might already be done in the system.</li> <li>• Can create false positives of different events potentially leading to some important events being ignored</li> </ul>	7	Level of response marking:	
				5 - 7 marks	<p>Candidate has evaluated the use of monitoring systems. Both positive AND negative benefits of the use of a monitoring system have been analysed and the candidate is able to make informed and appropriate judgements within the context provided. An implied conclusion is present which is informed by the supporting analysis.</p> <p>Subject specific terminology and knowledge will be clearly used to support and inform the explanations/evaluations.</p>
				3 – 4 marks	<p>Candidate has described the use of monitoring systems. Positive OR negative benefits of monitoring systems have been described and the candidate is able to make some judgements within the context provided.</p> <p>Some subject specific terminology and knowledge will be used.</p>
				1 – 2 marks	<p>Candidate has identified benefits (positive OR negative) of using monitoring systems.</p> <p>At the bottom of the mark band the candidate may have simply provided a single point about what a monitoring system does.</p>
				0 marks	Nothing worthy of credit.

Question	Answer	Marks	Guidance										
4	2 from, 2 marks each:  Confidentiality <ul style="list-style-type: none"> <li>• Only those authorised (1) can gain access (1)</li> <li>• Kept secure (1) from unauthorised users (1)</li> </ul> Integrity <ul style="list-style-type: none"> <li>• Maintaining the completeness of data (1)</li> <li>• Not allowing data to be modified in an unauthorised manner (1)</li> <li>• Assurance that the information is trustworthy/accurate (1)</li> <li>• Making sure the data is free from tampering (1)</li> </ul>	4											
5 (a)	1 mark each:  <table border="1" data-bbox="454 695 1151 1075"> <thead> <tr> <th data-bbox="454 695 763 762">Description of Attacker</th> <th data-bbox="763 695 925 762"></th> <th data-bbox="925 695 1151 762">Type of Attacker</th> </tr> </thead> <tbody> <tr> <td data-bbox="454 762 763 868">Use someone else's codes to hack into the computer</td> <td data-bbox="763 762 925 868" rowspan="3" style="text-align: center; vertical-align: middle;">  </td> <td data-bbox="925 762 1151 868">Phisher</td> </tr> <tr> <td data-bbox="454 868 763 970">Sells information on weaknesses in computer systems</td> <td data-bbox="925 868 1151 970">Script Kiddie</td> </tr> <tr> <td data-bbox="454 970 763 1075">Send an email pretending to be from the organisation</td> <td data-bbox="925 970 1151 1075">Vulnerability Broker</td> </tr> </tbody> </table>	Description of Attacker		Type of Attacker	Use someone else's codes to hack into the computer		Phisher	Sells information on weaknesses in computer systems	Script Kiddie	Send an email pretending to be from the organisation	Vulnerability Broker	3	One mark per line.  If more than one line from description to attacker, 0 marks for both lines.  Allow other methods of linking – numbers etc.
Description of Attacker		Type of Attacker											
Use someone else's codes to hack into the computer		Phisher											
Sells information on weaknesses in computer systems		Script Kiddie											
Send an email pretending to be from the organisation		Vulnerability Broker											
(b)	1 from: <ul style="list-style-type: none"> <li>• Hacktivist (1)</li> <li>• Cyber-criminal (1)</li> <li>• Insider (1)</li> <li>• Scammer (1)</li> <li>• Cyber-terrorist (1)</li> </ul>	1	CAO  Do NOT allow Phisher Script Kiddie Vulnerability Broker										

**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](mailto:general.qualifications@ocr.org.uk)

[www.ocr.org.uk](http://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 2022

