Cambridge Technicals
IT

Unit 3: Cyber Security

Level 3 Cambridge Technical in IT

Mark Scheme for January 2019

Oxford Cambridge and RSA Examinations

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.

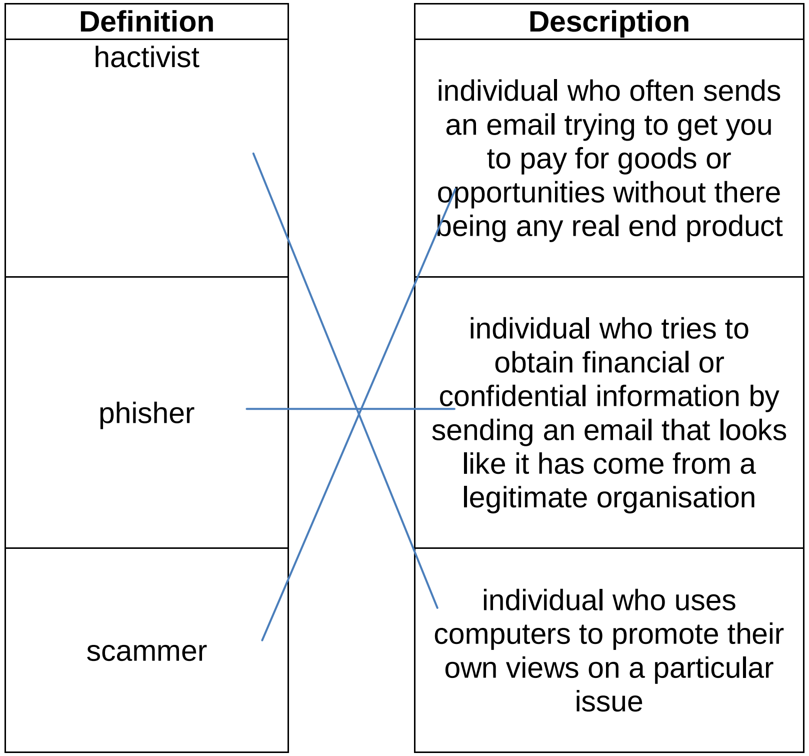
All examiners are instructed that alternative correct answers and unexpected approaches in candidates' scripts must be given marks that fairly reflect the relevant knowledge and skills demonstrated.

Mark schemes should be read in conjunction with the published question papers and the report on the examination.

Annotations - These are the annotations to be used when marking Unit 2:

Annotation	Meaning
✓	Tick – correct answer
✗	Cross – incorrect answer
➕	Plus – use for positives
➖	Minus – use for negatives
L1	Level 1
L2	Level 2
L3	Level 3
BOD	Benefit of doubt (This **does not** count as a mark – so 'tick' as well)
^	Omission mark
TV	Too vague
Rep	Repeat
SEEN or ⌇	Noted but no credit given

Section A

Question			Answer	Marks	Guidance
1	(a)		 Definition hactivist phisher scammer Description individual who often sends an email trying to get you to pay for goods or opportunities without there being any real end product individual who tries to obtain financial or confidential information by sending an email that looks like it has come from a legitimate organisation individual who uses computers to promote their own views on a particular issue	3	***For three marks.*** If more than three lines, then work from top to bottom of definition marking first three only.

<table>
<tr><th colspan="3">Question</th><th>Answer</th><th>Marks</th><th>Guidance</th></tr>
<tr><td><b>1</b></td><td><b>(b)</b></td><td></td><td><b>Possible reasons why Mr Thapa would want to keep his phone secure include:</b><ul><li>To protect his bank details (1) and prevent money being stolen (1).</li><li>To protect his photographs (1) and avoid identity theft (1).</li><li>To prevent his passwords being stolen (1) and orders being placed on his online account (1).</li><li>Any other valid suggestion.</li></ul></td><td>2</td><td><b><i>Up to two marks for valid explanation.</i></b>
Allow mix and match.
What can be done with his phone/information gathered from his phone.
To prevent confidential information/personal information/sensitive is TV needs to be exemplified for mark to be awarded.</td></tr>
<tr><td><b>1</b></td><td><b>(c)</b></td><td></td><td><table><tr><th>Characteristic</th><th>Script kiddie</th></tr><tr><td>age</td><td>mid teens – mid 30’s (1)</td></tr><tr><td>location</td><td>anywhere with an internet connection/home (1)</td></tr><tr><td>social group</td><td>online groups/like minded educational ability (1)</td></tr></table><ul><li>Any other valid suggestion in all cases.</li></ul></td><td>3</td><td><b>For three marks.</b>
Allow reasonable responses
For social group, do not accept character personality</td></tr>
</table>

Question			Answer	Marks	Guidance
1	(d)		**Indicative Content:** • Cafés invariably have lax security standards, meaning that anyone using these networks will be potentially vulnerable. • Busy, fast paced environment. Individuals more vulnerable to shoulder surfing activities, etc. • Individuals more easily distracted in environment. More opportunities for these vulnerabilities to be exploited. • Environment where individuals are more likely to use mobile devices so by nature there are more opportunities to target data, etc. • Crowded areas. Lots of customers. A perfect environment for targets of cyber security to be exploited. • People leave behind mobile devices/forget them. Only need a small window to exploit individual vulnerabilities. • Automated connection to WiFi • Not being aware of risks and/or protection software • People doing online banking using free WiFi • Being a foreigner and a tourist and shopping online • Any other valid suggestion.	7	**Level 3 [5-7 marks]** The learner has explained the reasons why people, such as Mr Thapa, can be targets of cyber security attacks in a coffee shop environment. Subject specific terminology and knowledge will be clearly used to support and inform the explanations. **Level 2 [3-4 marks]** The learner has described the reasons why people, such as Mr Thapa, can be targets of cyber security attacks in a coffee shop environment. **Level 1 [1-2 marks]** The learner has identified generic points why individuals can be targets of cyber security attacks. Subject specific terminology may be limited or missing. **0 marks = Nothing worthy of credit.**

Question			Answer	Marks	Guidance
1	(e)		**Possible methods that could be used by attackers to access Mr Thapa's phone include:** • Malware (1) Mr Thapa could be duped into downloading the malware (1) as it is often disguised (1). • Phishing (1) Mr. Thapa could be asked to go to a URL to enter information (1) which could result in disclosure of sensitive, personal information (1). • Use software vulnerability (1) a bug in the operating system (1) allows remote access (1). • Connected to Wi-Fi (1) all data sent/received is collected (1) and login credentials can be used (1). • Get the user to download a spy app (1) allows remote access to the phone (1) and all features (1). • Any other valid suggestion.	3	***Up to three marks for valid description.*** Allow mix and match Method must result in information/data being accessed, so DOS not suitable
1	(f)		**Possible ways Mr Thapa's life could be disrupted by cyber criminals using the information obtained from the phone hack include:** • Identity theft (1) opening credit card accounts/ applying for mortgages in his name (1). • Financial theft (1) stealing money from his bank account (1). • Social issues (1) posting unpleasant comments on social media pretending to come from him (1).	6	***Up to two marks for each of three descriptions.*** Three from list. MAX two marks per way.

Question			Answer	Marks	Guidance
			• Blackmail (1) photos on his phone he would not want made public (1). • Commit physical theft (1) as they know his home address (1) • Any other valid suggestion.		
1	(g)		**Possible access controls Mr Thapa could implement to secure his phone include:** • Passcode (1) a string of characters used to gain access to a computer or smartphone (1). • Fingerprint recognition (1) automated method of confirming the identity of Mr Thapa (1). • Face recognition (1) matches Mr Thapa's face to one on record (1). • Two factor authentication (1) use of a second device to authenticate (1) • Any other valid suggestion.	4	***Up to two marks for each of two descriptions.*** Two from list. MAX two marks per access control. MUST be about access control not securing the phone.

Question			Answer	Marks	Guidance
2	(a)		**Possible pieces of information Mr Thapa needs to provide to the cyber security team along with appropriate reason why needed include:** • Date/time of incident (1) to know which logs to look at (1). • Description of incident (1) to understand what happened (1). • Information accessed (1) to know the motivation of the hacker (1). • Security on phone (1) to know the capability of the hacker (1). • Mr Thapa contact details (1) for follow up questions/send report (1) • Any other valid suggestion.	6	***In each case:*** ***One mark for identifying a piece of information that Mr Thapa needs to supply and one mark for why this is needed by the cyber security team.*** Three from list. MAX two marks for each piece of information and reason why needed. Incident category and incident severity will NOT be provided by Mr Thapa but determined by the security team.
2	(b)		**Possible reasons why it is important to Mr Thapa that each member of the cyber security team has a different role include:** • A question is only asked once (1) so Mr Thapa's time is not wasted (1). • So Mr Thapa knows the focus of the questions (1) and can give appropriate responses (1). • So all areas of the investigation are covered (1) and all information from Mr Thapa is obtained (1).	2	***Up to two marks for valid explanation.*** For full marks, must be related to why it is important to Mr Thapa.

Question			Answer	Marks	Guidance
			• Mt Thapa might have a rapport with different members of the team (1)and give more information to them (1) • Report will be finished quicker (1) so damage to Mr Thapa's account can be limited (1) • Any other valid suggestion.		
2	**(c)**		**Possible ways that the coffee shop could use the review of the incident created by the cyber security team include:** • To train their staff (1) to look out for methods used by attackers (1). • To produce notices for customers (1) highlighting ways that can avoid being attacked (1). • To promote cyber security amongst their customers (1) improving their reputation/increasing customers (1). • To learn lessons from the incident (1) and ensure the appropriate safeguards are built into future working practices (1). • To use it as a reference (1) if any similar incidents happen again (1) • To see where potential vulnerabilities are in their network (1) and apply fixes (1) • Any other valid suggestion.	4	***Up to two marks for each of two valid explanations.*** Two from list. Max two marks per way.

Section B

Question			Answer	Marks	Guidance
3			**Possible ways of how cyber security aims to protect the confidentiality, integrity and availability of data include:** Confidentiality • Restricting access to those who need to know (1). • Example: limited personal photos to family only / encryption/passwords/tired access (1). • Any other valid suggestion. Integrity • Level of assurance which can be given to the data/how trustworthy it is/accuracy of data/ uptodate / only those authorised can update (1). • Example: Storing single copy of customer address (1). • Any other valid suggestion. Availability • When required data is present and can be used (1). • Example: Sales records are online when required (1). • Any other valid suggestion.	6	**For each of confidentiality, integrity and availability of data:** **One mark for valid description and one mark for valid example.** If no example, then max one per term.

Question			Answer	Marks	Guidance
4	(a)*		**Indicative Content:** • Use of NIDS does not degrade the performance of the system allowing other tasks to run without interruption. • Monitors are transparent making it difficult for attackers to locate and nullify it. • Only requires storage space, which is fairly cheap so older equipment could be used rather than purchase new equipment. • They are independent of the operating systems being used so can be used anywhere on the network. • They can be moved around the network targeting specific areas where there are known issues. • Can create alerts of potential attack allowing time to react. • Any other valid suggestion.	10	**Level 3 [7-10 marks]** The learner has explained why the use of NIDS is effective in protecting the information on the server. The explanation is supported by a clear and rationale argument related to effectiveness. Subject specific terminology and knowledge will be clearly used to support and inform the explanations. *There is a well-developed line of reasoning which is clear and logically structured. The information presented is relevant and substantiated.* **Level 2 [4-6 marks]** The learner has described the use of NIDS in protecting the information on the server but there is opportunities to weigh up the effectiveness of this system are missed. **Level 1 [1-3 marks]** The learner has identified generic points related to NIDS. Subject specific terminology may be limited or missing. **0 marks = Nothing worthy of credit.**

Question			Answer	Marks	Guidance
4	**(b)**		• Host Intrusion Detection System (HIDS) (1). • Anti virus software (1). • Signature based IDS (1). • Anomaly based IDS (1). • Intrusion Prevention System (IPS) • Any other valid suggestion.	1	**For one mark.** Do not allow IDS.
5			**Possible reasons why it is not possible to remove all risk include:** • Not all the risks are known (1) given the uncertainty of a business environment (1) so cannot remove what you don't know (1). • Some risks are required (1) to enable the business to operate (1) so cannot be removed (1). • Attackers will find new ways to exploit (1) always new hack methods being developed (1) • Attacker may be an insider (1) and needs access as part of their job (1) • Systems involve humans (1) who are unreliable/human error/do not follow rules (1) • Any other valid suggestion.	3	**Up to three marks for valid explanation.**

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