OCR
Oxford Cambridge and RSA

CAMBRIDGE TECHNICALS LEVEL 3 (2016)

Examiners' report

IT

05838−05842, 05877

Unit 3 January 2022 series

Contents

Introduction

Our examiners' reports are produced to offer constructive feedback on candidates' performance in the examinations. They provide useful guidance for future candidates.

The reports will include a general commentary on candidates' performance, identify technical aspects examined in the questions and highlight good performance and where performance could be improved. The reports will also explain aspects which caused difficulty and why the difficulties arose, whether through a lack of knowledge, poor examination technique, or any other identifiable and explainable reason.

Where overall performance on a question/question part was considered good, with no particular areas to highlight, these questions have not been included in the report.

A full copy of the question paper and the mark scheme can be downloaded from OCR.

Would you prefer a Word version?

Did you know that you can save this PDF as a Word file using Acrobat Professional?

Simply click on **File > Export to** and select **Microsoft Word**

(If you have opened this PDF in your browser you will need to save it first. Simply right click anywhere on the page and select **Save as . . .** to save the PDF. Then open the PDF in Acrobat Professional.)

If you do not have access to Acrobat Professional there are a number of **free** applications available that will also convert PDF to Word (search for PDF to Word converter).

Unit 3 series overview

This unit is mandatory for the Extended Certificate, Diploma and Extended Diploma and optional for all pathways for the Introductory Diploma and Foundation Diploma.

The unit focuses on:

- An understanding of cyber security and the issues surrounding it
- Measures that can be used to protect against cyber security incidents
- An understanding of how to manage cyber security incidents.

The paper is divided into two sections – A and B. Section A is worth 60% (40 marks) and are based around a pre-release scenario. The pre-release contains areas for further research that the candidate is expected to undertake and which form the basis of the questions to be asked. Section B is worth 40% (20 marks) and each question has its own short scenario.

Candidates who did well on this paper generally did the following:	Candidates who did less well on this paper generally did the following:
- Used technical terms - Related their responses to the scenario in the question - Used the keywords in the question to give appropriate depth to their response.	- Answered the question they thought was being asked, not the one actually being asked - Repeating the same point several times in different ways - Giving a response that has been eliminated in the question.

Section A overview

The pre-release identifies key research topics that the candidates should have spent some time working on. They need to have cross referenced the topics against the specification.

Question 1 (a) (i)

1   **(a)**   When E James installed the password manager app, the app gave some hints and tips on how to secure their phone including how to prevent access to the data stored on their phone.

Two of the hints and tips they were given were to:

- make sure that their phone is running the latest operating system (OS) by installing updates

- install an anti-malware app.

     (i)   Explain how each of these protect their data.

OS Updates ....

....

....

....

....

....

Anti-malware ....

....

....

....

....

....

[4]

The focus is on how these measures protect data. Any reference made by candidates to OS updates adding new features was not credited. Many did identify that an update would patch an existing vulnerability and gained marks. There are many aspects to anti-malware which allow it to protect data and candidates were generally confident in their explanations.

Question 1 (a) (ii)

(ii) Identify and explain **two** other methods that could be used to prevent access to data stored on the phone.

Method 1 ....

....

Description ....

....

....

....

....

....

Method 2 ....

....

Description ....

....

....

....

....

....

[6]

OS Updates and Anti-malware were in the previous question. This one asked for two **other methods**, this meant that OS Updates and Anti-malware could not gain any marks. A significant number of candidates wrote about these. Candidates who did give suitable methods did not develop their responses with additional detail and often did not gain the subsequent marks.

?	**Misconception**	A common misconception is that encryption makes the data unreadable. The data is still readable, but meaningless.

Question 1 (b) (i)

(b) (i) Two types of cyber security incident that could be caused by an individual obtaining the passwords that are stored in the password manager are account lockout and destruction.

Describe these types of cyber security incident.

Account Lockout ....

....

....

....

....

....

Destruction ....

....

....

....

....

....

[4]

A large number of responses repeated the question – account lockout is where the account is locked. This, unfortunately, does not demonstrate any knowledge or understanding. Many candidates correctly identified that account lockout means no access but did not go beyond that. Likewise, destruction was linked to deleted/destroyed but nothing more to gain the second mark.

Question 1 (b) (ii)

(ii) Identify **one** other type of cyber security incident that could be caused by an individual obtaining the passwords stored in the password manager.

....

.... **[1]**

The list of cyber security incidents that were acceptable are listed in the specification. This was a knowledge regurgitation question and many candidates gained the mark. It was unfortunate that there was a small number of candidates who gave either account lockout or destruction even though they were excluded by the question.

Question 1 (c)

(c) Threats to the data stored on E James's phone can be classified as accidental or intentional.

Describe what is meant by an accidental and an intentional cyber security threat.

Accidental ....

....

....

....

....

....

Intentional ....

....

....

....

....

....

[4]

This question was answered very well with the majority of candidates demonstrated a good knowledge and understanding of the difference. Those that gave examples to demonstrate their understanding were more likely to achieve the second mark.

Question 1 (d)

(d) Describe **two** methods that could be used during a cyber attack, to obtain the passwords stored in the password manager.

1 ....

....

....

....

....

....

2 ....

....

....

....

....

[4]

The focus of the question is not on obtaining generic data but specifically, the passwords in the password manager. Answers, such as change the password do not answer the question. Answers that focused on backups or storing in the cloud also did not gain credit. Many identified the method but did not describe it, instead giving advantages of its use.

Question 1 (e) (i)

(e) A cyber security attack has taken place and E James is advised that they need to reduce the impact of the theft of the passwords.

   (i) Describe **one** action that could be made to reduce the impact of the theft of the passwords.

   ....

   ....

   ....

   .... **[2]**

Many candidates misinterpreted the question. A cyber security attack has taken place and the passwords have been stolen. The focus of the question is how to reduce the impact of the passwords being in the hands of the criminal. The majority gave responses on how to protect the account itself rather than focusing on the individual passwords that have been stolen.

Question 1 (e) (ii)

(ii) Explain how the action you have described above will reduce the impact.

....

....

....

....

....

.... **[3]**

Without giving a satisfactory response to the first part, candidates could not obtain marks here. Many candidates did not give a sensible, usable way of reducing the impact of the theft of the passwords and as a consequence were unable to explain how the action reduced the impact of the theft.

Question 1 (e) (iii)

(iii) Identify **one** other action E James could take.

....

.... **[1]**

A small minority of candidates repeated the action they gave in the first part of the question. This required a different action. As with 1e(i), many actions related to securing the password manager and not securing the accounts whose passwords had been stolen.

Question 2

2* Evaluate the ethical considerations of using a password manager.

[10]

....

....

....

....

....

....

The contents of the responses given was generally good and covered a range of ethical considerations. There was a lack of examination technique among the candidates which restricted the marks that they achieved. There was limited explanation of the points made. An evaluation requires both positive and negative explanations and a conclusion.

	AfL	Essays are marked using bands and not using points. This means that the candidate needs to be making a few points but each point needs to show the depth of their knowledge and understanding rather than many points which demonstrate a superficial breadth. A discussion requires an explanation, back up with examples relevant to the question. The explanation needs to make up the majority of the response rather than be added as an afterthought.

Section B overview

This section is not based on the pre-release material. Each question is given a short context and candidates are expected to use it, where appropriate, within their responses.

Question 3 (a)

3   Padas Travel Company has suffered a cyber security incident. Its server was hacked and all customer information stolen. The information stolen included:

- Customer personal details
- Customer financial details
- Details about the holidays they have booked.

Following the cyber security incident, Padas Travel Company has hired a security company to produce a cyber security incident report about the theft of data.

(a)   Identify **two** areas that could have been impacted by the theft of the customer data.

1 ....

....

2 ....

....

[2]

Most candidates achieved full marks on this question.

Question 3 (b)

(b) Describe **two** items that need to be considered in the review section of the cyber security incident report.

1 ....

....

....

....

....

....

2 ....

....

....

....

....

....

[4]

A large number of candidates did not focus their response on the review section, instead choosing to give responses about the content of any section of the cyber security incident report. The review section appears at the end of the report and focuses on which parts of the plan worked and which did not – a theoretical plan against real world actions with recommendations for improvements.

Question 3 (c)

Following the publication of the cyber security incident report, Padas Travel Company has decided to investigate the use of monitoring systems as part of their cyber security risk management system.

(c)* Evaluate the use of monitoring systems as a method of cyber security risk management.

....

....

....

....

....

.... **[7]**

Many candidates misread the question and so many candidates evaluated methods that were preventative rather than monitoring based and achieved low marks. Those that did focus on monitoring systems often did not give explanations and did not reach the top band. Many systems will both monitor and prevent and it was important that candidates restricted their response to the monitoring element only and explanations of the benefits and drawbacks of monitoring.

Question 4

4   Two of the objectives of security are maintaining confidentiality and integrity of data.

Describe what is meant by confidentiality and integrity.

Confidentiality ....

....

....

....

....

....

Integrity ....

....

....

....

....

....

[4]

This was answered very well. The majority of candidates gained both marks for confidentiality. Integrity was less well understood and answered by the candidates, but most managed to gain 1 mark.

Question 5 (a)

5   Companies are targeted by different types of attacker, each with their own separate agenda.

(a)   Draw a line to connect each description of an attacker to the correct type.

Description of Attacker
Uses someone else's codes to hack into the computer
Sells information on weaknesses in computer systems
Sends an email pretending to be from the organisation

Type of Attacker
Phisher
Script Kiddie
Vulnerability Broker

[3]

This was answered very well with the majority of candidates achieving full marks.

Question 5 (b)

(b)   Identify **one** other type of attacker.

....

.... **[1]**

Most candidates achieved the mark here. Candidates who did not gave one of the types of attacker from the previous question.

Supporting you

Review of results

If any of your students' results are not as expected, you may wish to consider one of our review of results services. For full information about the options available visit the OCR website.

Supporting you through 2021-2022

Our priority is supporting you and your students this spring and to support you as you prepare for summer 2022. We'll update our website information regularly with resources, guidance and key information.

Take a look at our support for:

- Teachers
- Students
- Exams officers

Keep up-to-date

We are sending a weekly roundup to tell you about important updates. You can also sign up for your subject specific updates. If you haven't already, sign up here.

OCR Professional Development

Attend one of our popular CPD courses to hear directly from a senior assessor or drop in to a Q&A session. All our courses for the academic year 2021-2022 are being delivered live via an online platform, so you can attend from any location.

Please find details for all our courses on the relevant subject page on our website or visit OCR professional development.

Signed up for Exambuilder?

ExamBuilder is the question builder platform for a range of our GCSE, A Level, Cambridge Nationals, Cambridge Technicals and Functional Skills qualifications. See the full list of available qualifications in the sign up form.

ExamBuilder is **free for all OCR centres** with an Interchange account and gives you unlimited users per centre. We need an Interchange username to validate the identity of your centre's first user account for ExamBuilder.

If you do not have an Interchange account please contact your centre administrator (usually the Exams Officer) to request a username, or nominate an existing Interchange user in your department.

Supporting you

Active Results

Review students' exam performance with our free online results analysis tool.

For the spring 2022 series, results analysis is available for Cambridge Nationals (moderated units) only.

It allows you to:

- review and run analysis reports on exam performance
- analyse results at question and/or topic level
- compare your centre with OCR national averages
- identify trends across the centre
- facilitate effective planning and delivery of courses
- identify areas of the curriculum where students excel or struggle
- help pinpoint strengths and weaknesses of students and teaching departments.

Find out more at ocr.org.uk/activeresults.