CAMBRIDGE TECHNICALS LEVEL 2 (2016)

Examiners' report

IT

05882, 05883, 05884

Unit 2 Summer 2019 series
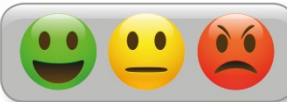
Version 1

Contents

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** > **Save As Other . . .** 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).

We value your feedback

We'd like to know your view on the resources we produce. By clicking on the icon above you will help us to ensure that our resources work for you.

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.

Note to Centres

There were a number of centres who had selected an invalid combination of units or had claimed the wrong units for a candidate that prevented overall qualifications results being issued. Please note that it is the responsibility of the centre to check that correct units have been entered for certification claims. OCR cannot guarantee that the issuing of results in these circumstances will meet deadlines for UCAS confirmation.

Sector Update

Two key changes have occurred in relation to the Level 3 Technicals qualifications, both in relation to the examined units; firstly, an additional re-sit has been allowed, so candidates can have 2 further attempts at an examined unit if they wish to improve their result from the first attempt made. And secondly, a 'near pass' R grade has been introduced, which enables candidates who do not pass but achieve sufficient marks to gain some points for their examined unit outcome, which may mean that it is not necessary to re-sit the exam.

Paper Unit 2 series overview

It was pleasing to see the improvement in the level of technical language from January maintained although there was a dip in understanding of the underlying principles of cyber security with many terms not clearly defined. Centres should make sure that candidates are familiar with all areas of the unit content before being entered for the external examination.

Section overview

To reiterate from the examiner's report in January, high marks require three elements: knowledge of the subject area, an understanding of the requirements of the keyword in the question and an application of the answer to the scenario. In many of the responses marked, one or more of these elements was missing. Candidates should be aware of the differing command words, e.g. identify, describe, explain, discuss, and the demands of each of these and how these command words require different depths of response. This was lacking in many responses. There is a teacher guide, available on the OCR website, on command verb definitions that gives the expectations of each one.

Question 1a

(a)   Social engineering is a term describing the act of manipulating people into giving out confidential information.

Identify **two** different types of social engineering.

1

2

[2]

This was done reasonably well with candidates able to identify two different forms of social engineering.

Question 1b

(b)   Identify the type of cyber security incident which occurs when school attendance records are changed by a cyber attacker.

[1]

These are listed in the specification and required a regurgitation of knowledge. Many candidates gave data manipulation instead of modification as their answer. These are basic definitions that should be learnt.

Question 1c

(c)   One motivation of a cyber attacker is publicity.

Identify **two other** possible motivations of a cyber attacker.

1 [   ]

2 [   ]

[2]

There are four motivations listed in the specification, one was identified in the question, this left two from a possible three. Many students did not achieve these simple low level marks due to a lack of knowledge. They should have a copy of the specification and at least know the terminology, this will allow them to access these basic marks.

Question 2a

The customer data of an online shopping website is stored in a database. The database is held on physical servers with a backup stored on the cloud.

A cyber security incident has occurred and some customers of this online shopping website have received emails relating to orders that they have not placed. The emails have asked the customers to reply with an email containing their login and financial details.

(a)   Identify and describe the type of cyber attack on the customers.

[4]

This comes from Section 2.1 of the specification – types of threat and whilst may could identify the type of attack, a description was less forthcoming. Many repeated the content of the question, redescribing what had happened without adding any further details or linking it to the question.

Question 2b

(b)   Identify the Act that has been broken during this cyber security incident.

[1]

This was a knowledge based question and it was pleasing to see that there was an increase in the number of students who correctly identified the Act from previous sessions.

Question 2c

(c)   Explain **two possible** impacts on the customers of this cyber security incident.

1

2

[6]

This was a higher level question. It was asking the candidate to explain what the impact was on the customer. Many gave general answers or repeated themselves and gave the same answer twice. As an explanation, the level of detail required in the answer is greater than a description and this is reflected in the number of marks. Candidates who did only write one line were not giving enough information to be able to access all of the marks.

Question 2d

(d)   The organisation uses 'token authentication' to try to protect the customer database.

Describe **one** characteristic of a token authentication protection measure.

[2]

This question was poorly answered. The majority of candidates seemed unaware of token authentication and gave answers based on two factor authentication instead.

Question 2e

(e)   Following the cyber security incident, the organisation is considering implementing an Access Management Policy.

Describe, using an example, what is meant by an Access Management Policy.

[3]

Very few candidates gave answers based around roles, responsibilities, username and access rights. The vast majority of responses seemed to be based around what they could access on the internet. Section 3.1 is an important one in understanding how to minimise the impact from cyber security incidents and an understanding of the terms and how they are applied is important.

Question 3a

Personal digital assistants are used in houses to play music, create shopping lists, order and pay for goods from online shopping websites. The devices can also be used to turn lights on and off and to control central heating. Personal digital assistants have access to personal information including location and debit/credit card details.

The devices use wireless connections to the internet access point, usually a router, in a house. Many internet access points have no security procedures when connecting to the internet.

(a)   Identify and describe **one** system vulnerability that could lead to a cyber security attack on the internet access point.

[3]

The question was focusing on a system vulnerability. It was unfortunate that a large number of candidates gave general vulnerabilities and in particular ones that were human related, missing the point of the question.

Question 3b

(b)   Identify and describe **one** individual threat that could occur to the internet access point.

[3]

Hacking was the most popular correct answer that was seen for this question, there were a few who gave DOS/DDOS but very few developed their answer to gain the description marks.

Question 3c

(c)   Malware could be downloaded and installed on the personal digital assistant.

Identify **two** different types of malware.

1

2

[2]

This was a knowledge regurgitation question and was answered very well with most identifying one type of malware and many, two.

Question 3d

(d)   Explain, using an example, how a firewall could be used to increase the security of the personal digital assistant.

[4]

Many candidates did not know what a firewall was or how it could be used to increase security. Very few candidates were able to explain how a firewall worked in any specific way or use technical language to do so.

Question 3e

(e)   Firewalls and token authentication are two logical protection measures.

Identify and describe **one** other logical protection measure that could be used to increase the security of the internet access point.

[3]

Passwords was the most common correct answer given here but as in many other questions, candidates did not apply examination technique and identify and fulfil the requirements of the keyword. Few expanded on passwords to describe how it would work.

Question 3f

(f)   Discuss the importance of cyber security for the personal digital assistant and the internet access point.

[9]

This question is marked using a level of response mark scheme. The low mark band is identification, the middle mark band is description and marks in the top band are given for discussion. The content is as important as meeting the requirements of the command word. Many candidates did not focus on the personal digital assistant nor did they explain why cyber security was important. These two elements were required for top band answers. There were many descriptions with the majority of candidates achieving mark band two with a small number merely listing.

It is important that the candidates are aware of the content and able to apply their knowledge and understanding to the context required but they must also look at the command word and make sure that there is sufficient depth in their response. The scattergun approach – identify as many points as possible will achieve a mark in the low mark band. The response being looked for is about depth of answer and not breadth.

Copyright information

Any reference to existing companies or organisations is entirely coincidental and is not intended as a depiction of those companies or organisations.

Supporting you

For further details of this qualification please visit the subject webpage.

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. If university places are at stake you may wish to consider priority service 2 reviews of marking which have an earlier deadline to ensure your reviews are processed in time for university applications.

Mark grade boundaries

Find the grade boundaries for this series on the OCR website.

CPD Training

Attend one of our popular CPD courses to hear exam feedback directly from a senior assessor or drop in to an online Q&A session.

Please find details for all our courses on the relevant subject page on our website.

www.ocr.org.uk

www.ocr.org.uk

OCR Customer Support Centre

Vocational qualifications
Telephone 02476 851509
Facsimile 02476 851633
Email vocational.qualifications@ocr.org.uk