CAMBRIDGE TECHNICALS

CAMBRIDGE TECHNICALS LEVEL 2 (2016)

Examiners' report

IT

05882, 05883, 05884

Unit 2 Summer 2022 series

Version 1

ocr.org.uk/cambridgetechnicals

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 2 series overview

This unit is mandatory for the Certificate and for the IT Practitioner and Digital Software pathways for the Diploma.

The unit focuses on:

- aspects of cyber security
- threats and vulnerabilities that result in cyber security attacks
- how impacts from cyber security attacks can be minimised.

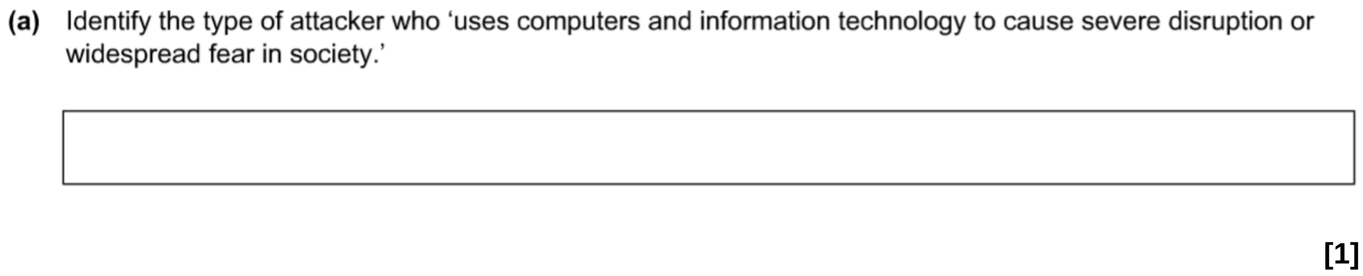
The questions in the paper are preceded by a scenario that involves an aspect of cyber security. The questions are based around this scenario. The paper may contain different scenarios for different questions.

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 responses.	• missed questions out • gave learnt responses from previous mark schemes that were not applicable • gave responses using identified keywords from other questions in the paper • used technical terms incorrectly.

There are large numbers of candidates who are not attempting all questions, and this is preventing them from accessing the higher grades.

Candidates need to learn the key words in the specification and their associated definitions and then apply them to the scenario. There is evidence that candidates are not familiar with the technical terms used in cyber security.

Question 1 (a)

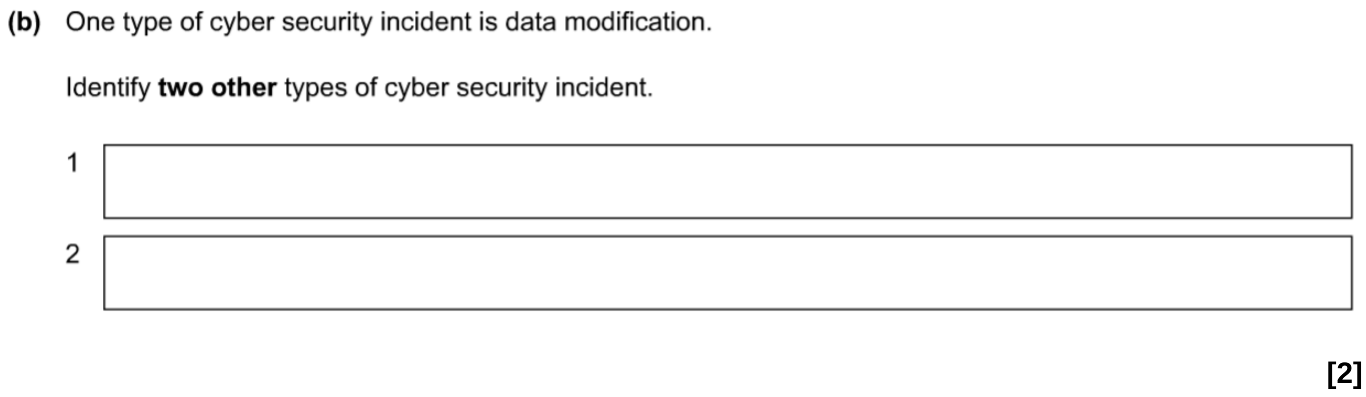


(a) Identify the type of attacker who 'uses computers and information technology to cause severe disruption or widespread fear in society.'

[1]

The specification lists a number of types of attackers and only one of those fitted the definition given above – cyber terrorist. Very few candidates gave the correct response.

Question 1 (b)



(b) One type of cyber security incident is data modification.

Identify **two other** types of cyber security incident.

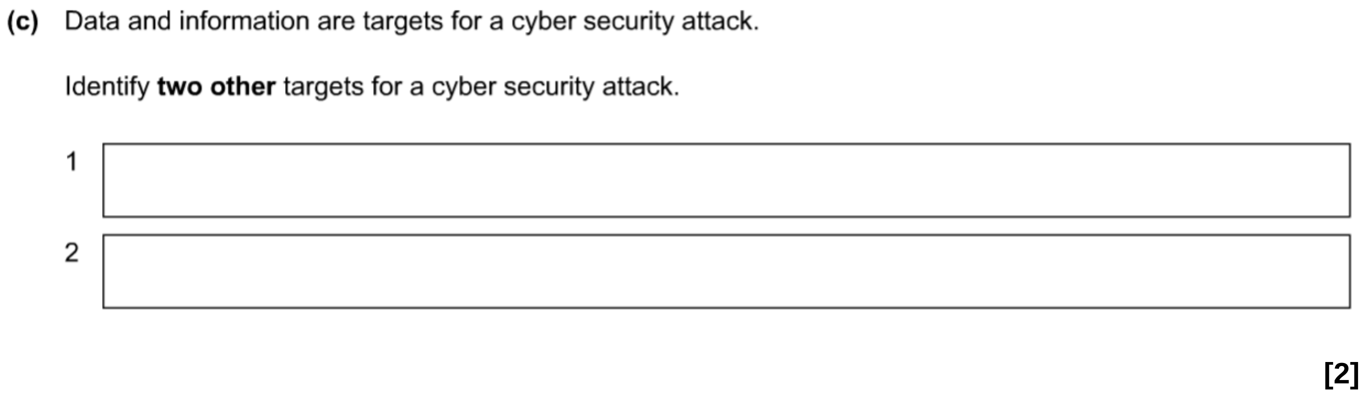
1

2

[2]

Candidates responded very well to this question with the majority scoring highly. It was disappointing to see some candidates giving data modification as one of their responses when this was given in the question.

Question 1 (c)



(c) Data and information are targets for a cyber security attack.

Identify **two other** targets for a cyber security attack.

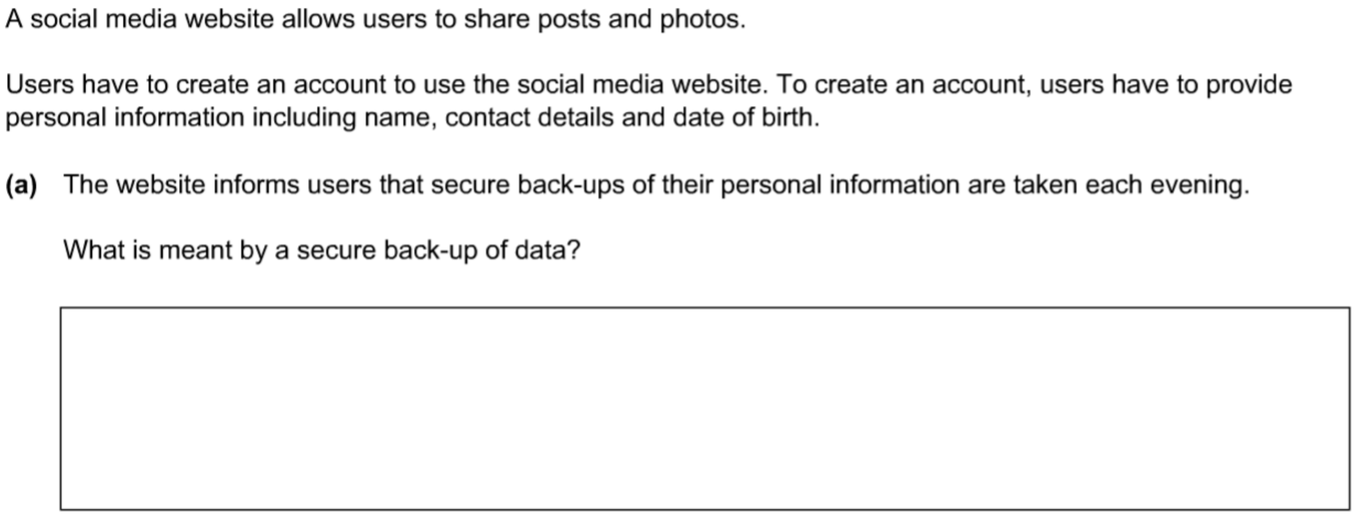
1

2

[2]

This question required a learnt response from the specification. As with the previous question, responses incorporated the data and information given in the question and so gained no marks.

Question 2 (a)



A social media website allows users to share posts and photos.

Users have to create an account to use the social media website. To create an account, users have to provide personal information including name, contact details and date of birth.

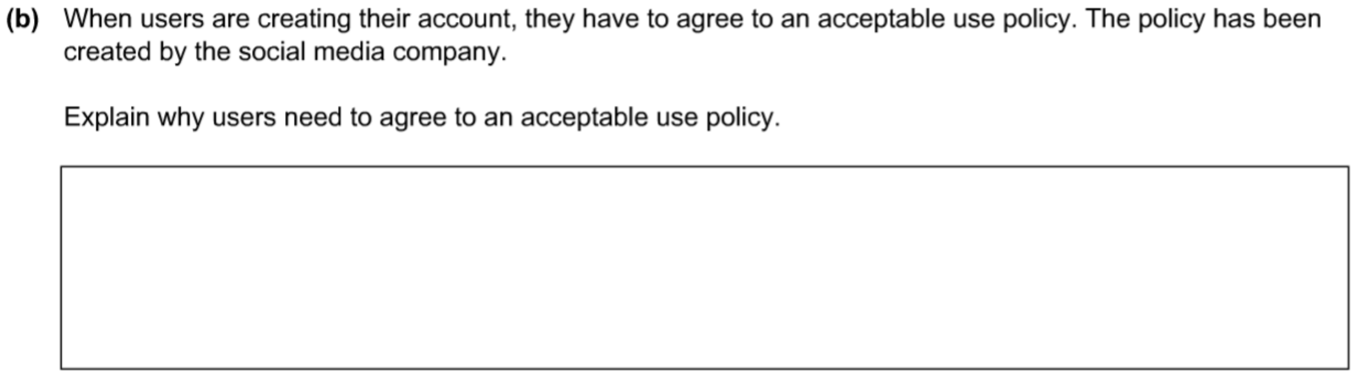
(a) The website informs users that secure back-ups of their personal information are taken each evening.

What is meant by a secure back-up of data?

[3]

When writing about backups, it is important that Candidates are clear that the backup is a copy of the original. Unless there is a clear indication that a second version exists then the candidate is not talking about a backup. Other key features of a backup include the good practice of keeping it away from the original – so off site. The secure element of the question was missing from many candidates' responses.

Question 2 (b)



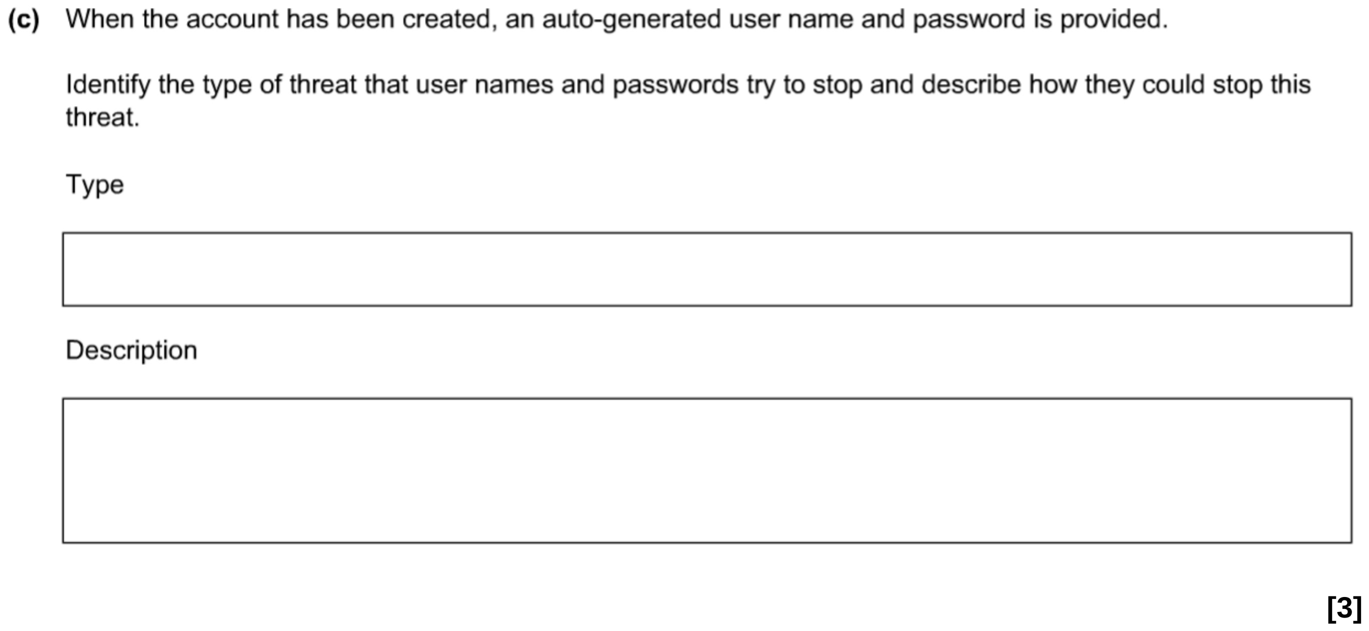
(b) When users are creating their account, they have to agree to an acceptable use policy. The policy has been created by the social media company.

Explain why users need to agree to an acceptable use policy.

[3]

On the surface this is a relative straight forward question. The AUP is provided by the social media company – many candidates answered this question by giving details on copyright and the social media being able to use the posts rather than what the users are and are not allowed to do. The key word in this question was "explain". This meant that some element of consequences was required.

Question 2 (c)



(c) When the account has been created, an auto-generated user name and password is provided.

Identify the type of threat that user names and passwords try to stop and describe how they could stop this threat.

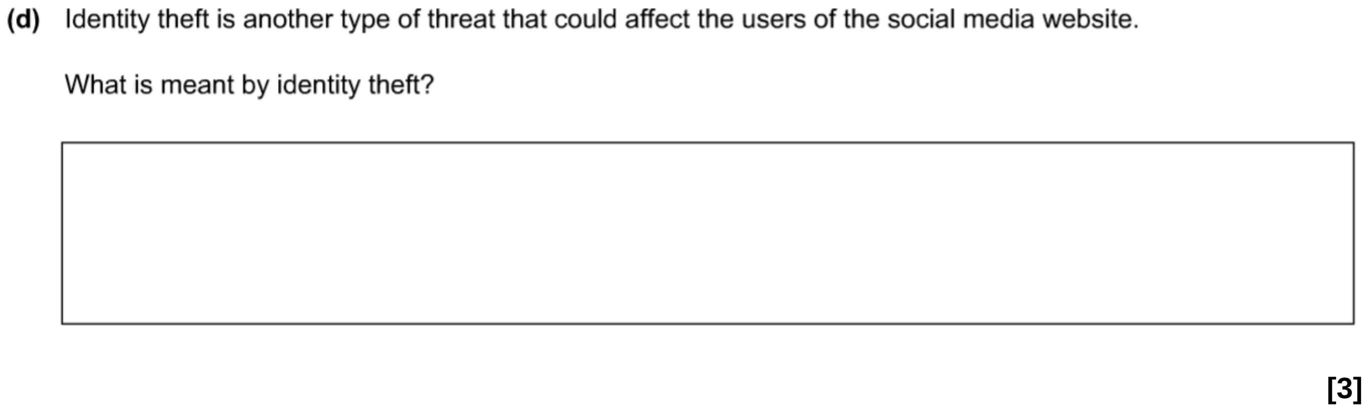
Type

Description

[3]

The first response required was the threat that is being stopped, followed by a description of the threat or how the username and passwords can prevent the threat – both variations were accepted. Few candidates gave an appropriate type of threat and so were unable to gain marks in this question. A large proportion gave identity theft, which is the focus of Question 2(d).

Question 2 (d)



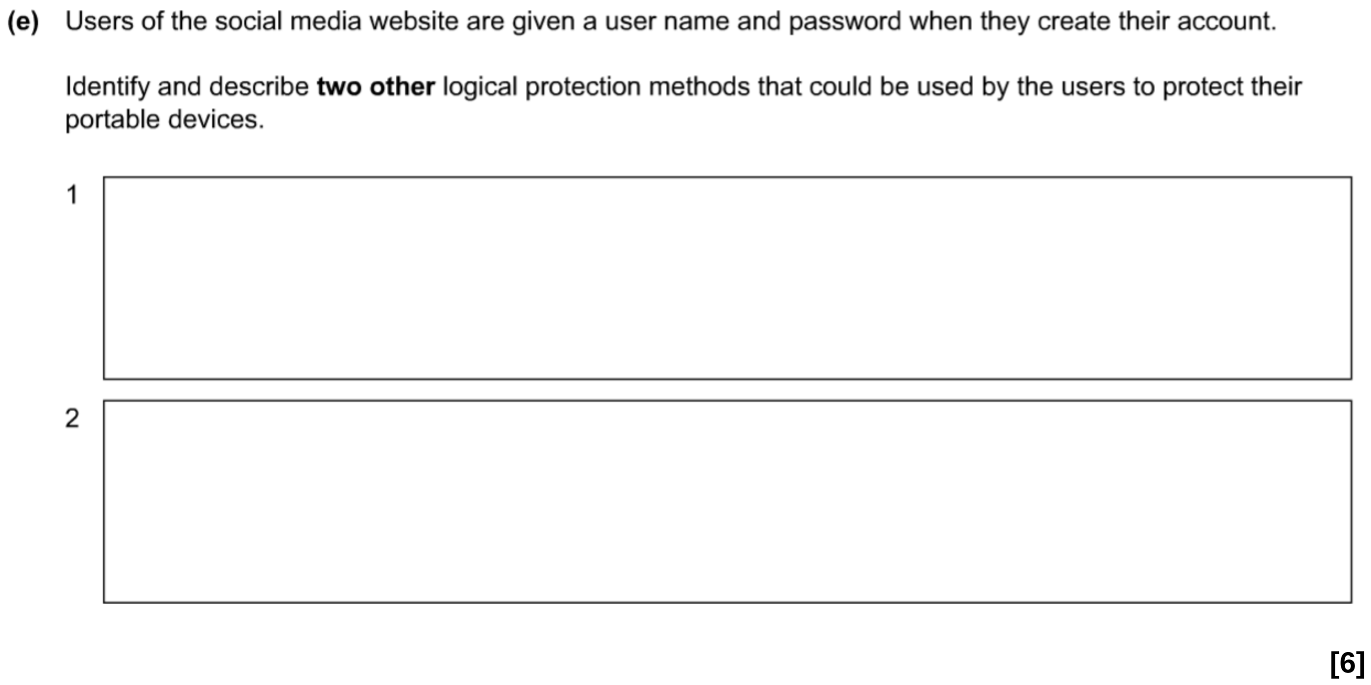
(d) Identity theft is another type of threat that could affect the users of the social media website.

What is meant by identity theft?

[3]

A majority of candidates answered this question very well and were able to achieve high marks.

Question 2 (e)



(e) Users of the social media website are given a user name and password when they create their account.

Identify and describe **two other** logical protection methods that could be used by the users to protect their portable devices.

1

2

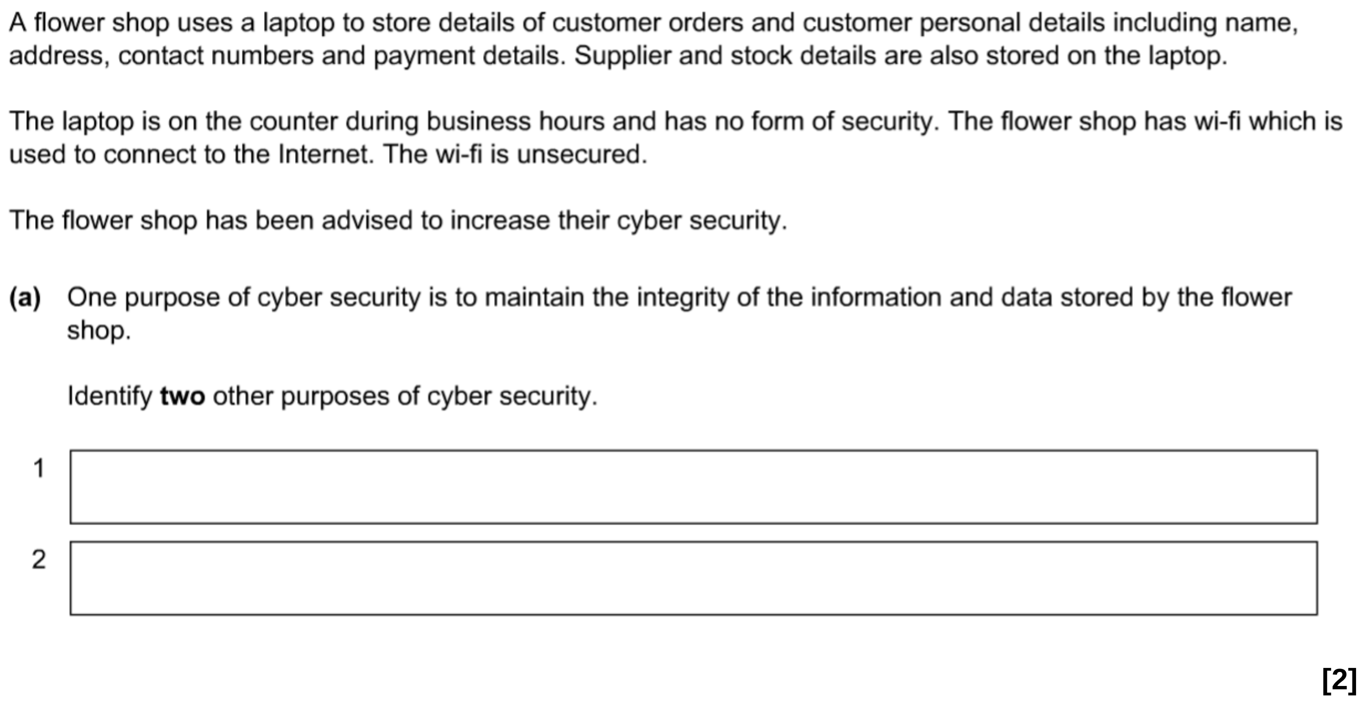
[6]

As with previous questions, there was a large number of candidates who gave a response that was given in the stem of the question – usernames/passwords. Identifying the method was somewhat successful for many, but the description of the method was lacking.

Misconception

The difference between logical and physical protection is an important one and candidates need to know the difference and the types of methods that fit into each category.

Question 3 (a)



A flower shop uses a laptop to store details of customer orders and customer personal details including name, address, contact numbers and payment details. Supplier and stock details are also stored on the laptop.

The laptop is on the counter during business hours and has no form of security. The flower shop has wi-fi which is used to connect to the Internet. The wi-fi is unsecured.

The flower shop has been advised to increase their cyber security.

(a) One purpose of cyber security is to maintain the integrity of the information and data stored by the flower shop.

Identify **two** other purposes of cyber security.

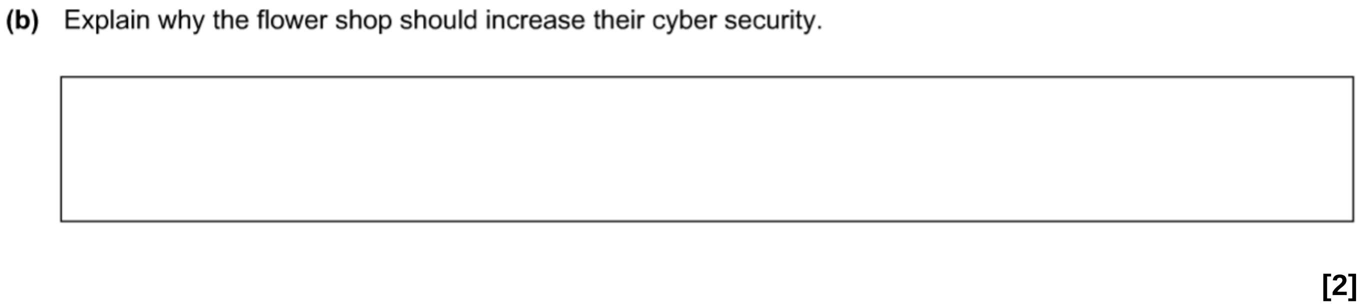
1

2

[2]

This question required a learnt response from the specification. As with previous questions, responses incorporated information given in the question – integrity of information and so gained no marks.

Question 3 (b)

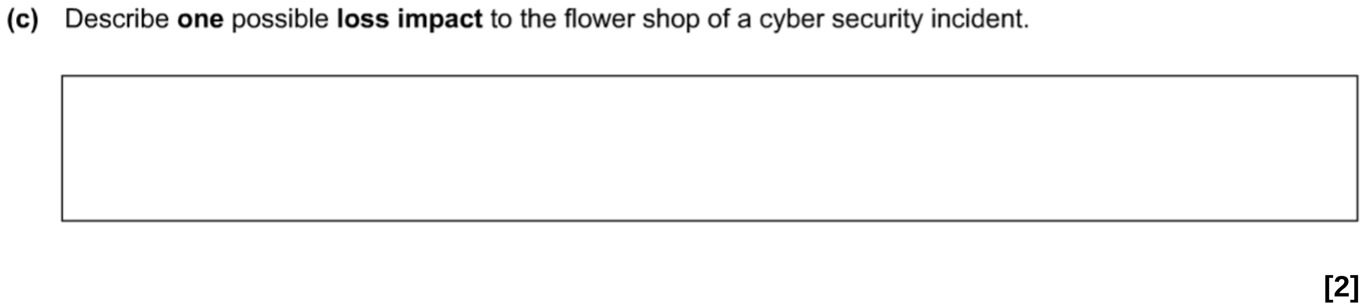


(b) Explain why the flower shop should increase their cyber security.

[2]

Candidates responded very well to this question with the majority gaining high marks. There was a large degree of contextualisation which was very good to see and contributed to the high marks achieved.

Question 3 (c)

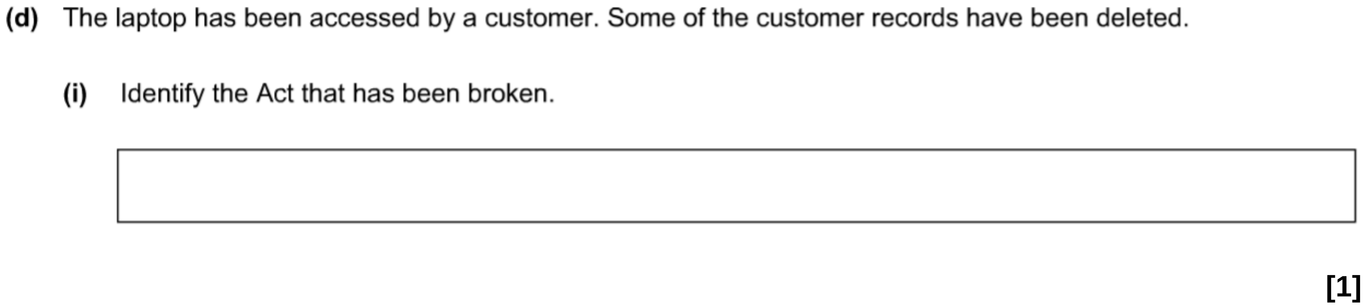


(c) Describe **one** possible **loss impact** to the flower shop of a cyber security incident.

[2]

The focus of the question was on the impact to the flower shop – this means it needs to be a tangible impact that can be measured. Many responses were very non-descript and vague without giving key points. A description needs to start with an identification and then build on that. A lack of examination technique is hindering the candidates from accessing higher marks.

Question 3 (d) (i)



(d) The laptop has been accessed by a customer. Some of the customer records have been deleted.

(i) Identify the Act that has been broken.

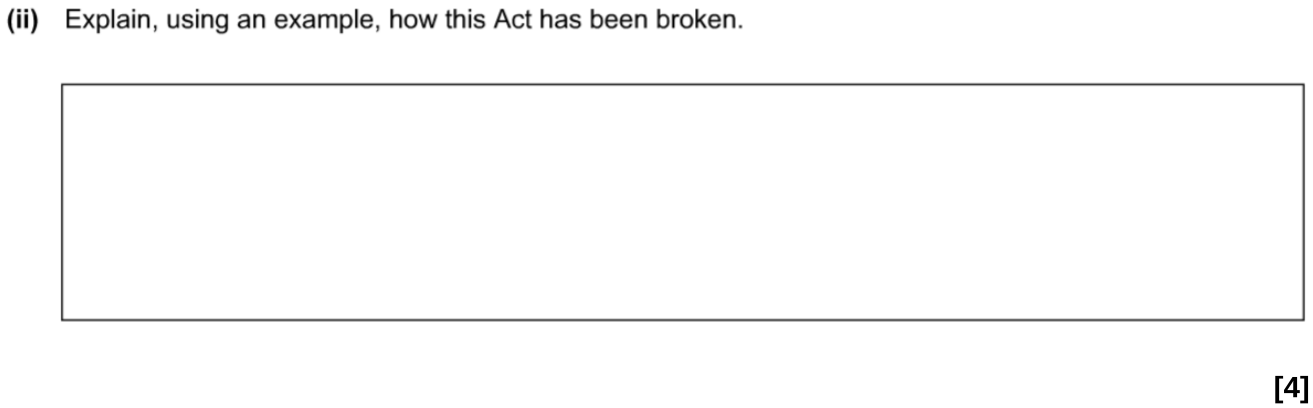
[1]

This was a learnt response based on the information given but was unfortunately not done very well. The majority of incorrect responses being the Data Protection Act – which was the response to a question from January.

Assessment for learning

The difference between the various Acts and what and how they apply needs to be known. With many questions being follow on from the correct identification of the law a large number of marks can be easily lost or gained.

Question 3 (d) (ii)

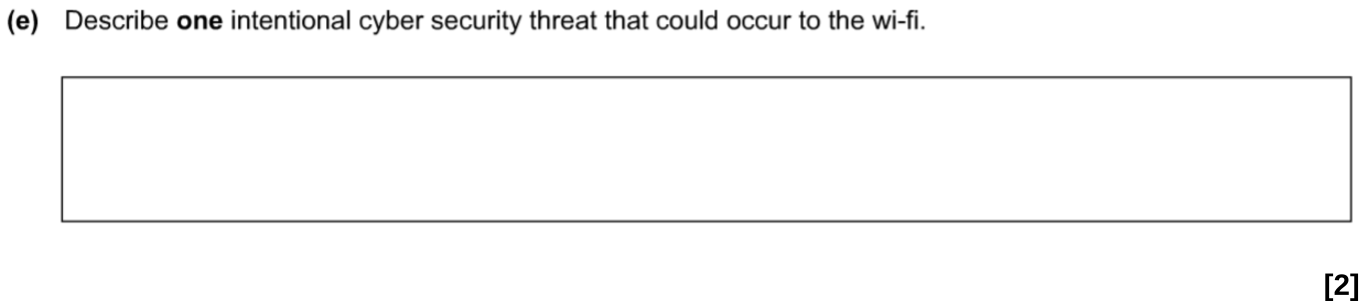


(ii) Explain, using an example, how this Act has been broken.

[4]

Without successfully identifying the act in the previous question, marks could not be gained here. Those who did identify the Computer Misuse Act went on to score very well.

Question 3 (e)

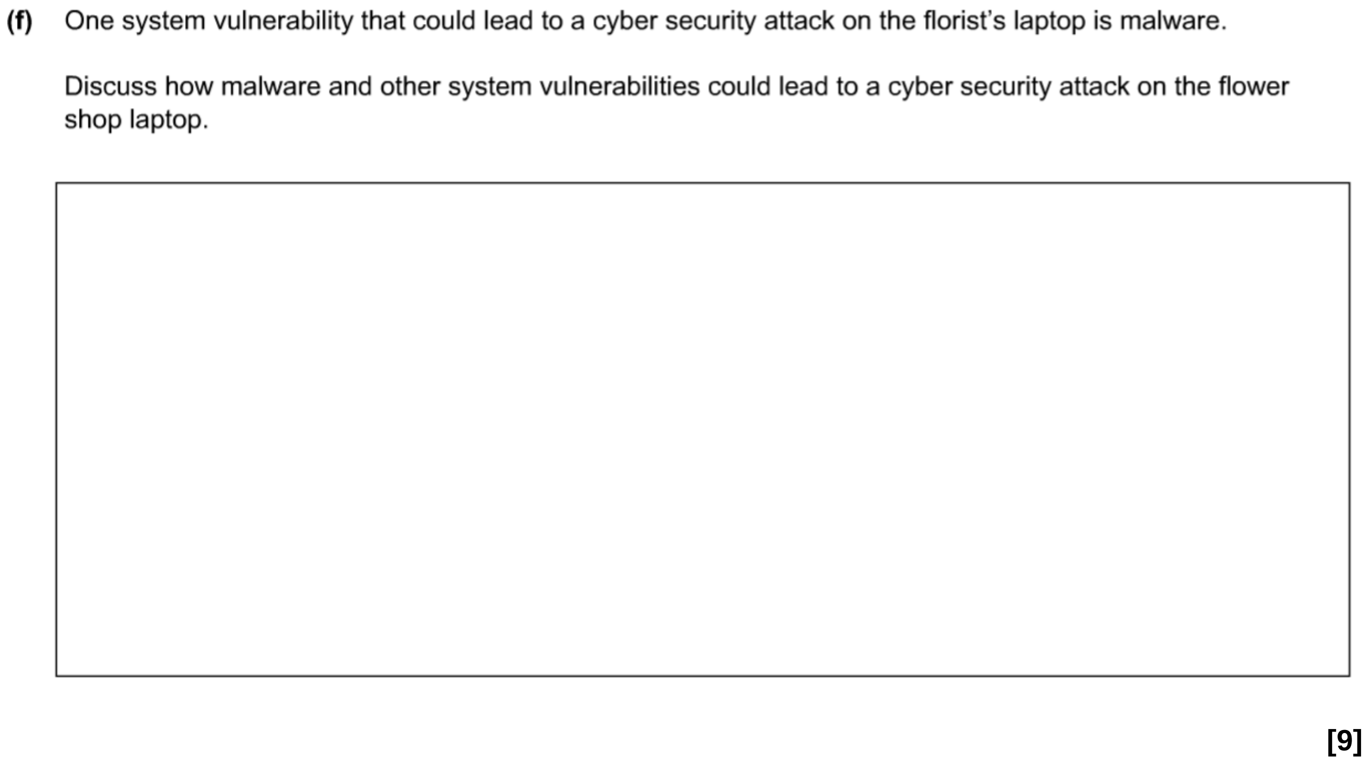


(e) Describe **one** intentional cyber security threat that could occur to the wi-fi.

[2]

The focus of the question was on the wi-fi and the specific threat that it was vulnerable to. This required the candidate to do two things – to be able to regurgitate the learnt knowledge from the specification on the different types and cyber security threats and then to filter those to the ones that would be applicable to wi-fi. Without successfully achieving the first, no marks could be gained on the second. The most common responses were hacking, DDOS and theft – all correct, however candidates often did not gain the second mark because their description was not in enough detail.

Question 3 (f)



(f) One system vulnerability that could lead to a cyber security attack on the florist's laptop is malware.

Discuss how malware and other system vulnerabilities could lead to a cyber security attack on the flower shop laptop.

[9]

The final question on this paper has consistently been an essay. Essays require a longer response from the candidate that is planned to take into account the context of the question and the keyword.

The focus of the question was how system vulnerabilities would lead to a cyber security attack. A significant proportion of candidates gave responses that related to the different types of system vulnerabilities and malware that could affect the flower shop rather than looking at how these vulnerabilities could be exploited.

Assessment for learning

Essays, such as this require depth of response from the candidate rather than breadth. A few points are required but the candidate is required to show their understanding of the point and its application to the question. Formatting their response can assist this, with each point being made being a separate paragraph; this can help focus the candidate on the point being made rather than moving onto a different one and reducing the depth of their argument and marks given.

Supporting you

Post-results services

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

Keep up-to-date

We send 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. Most of our courses are 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 and Cambridge Technicals qualifications. Find out more.

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.

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
/ocrexams
/ocrexams
/company/ocr
/ocrexams

We really value your feedback

Click to send us an autogenerated email about this resource. Add comments if you want to. Let us know how we can improve this resource or what else you need. Your email address will not be used or shared for any marketing purposes.

👍 **I like this** 👎 **I dislike this**

Please note – web links are correct at date of publication but other websites may change over time. If you have any problems with a link you may want to navigate to that organisation's website for a direct search.

CAMBRIDGE
UNIVERSITY PRESS & ASSESSMENT