CAMBRIDGE TECHNICALS

OCR
Oxford Cambridge and RSA

CAMBRIDGE TECHNICALS LEVEL 2 (2016)

Examiners' report

IT

05882, 05883, 05884

Unit 2 January 2021 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 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.

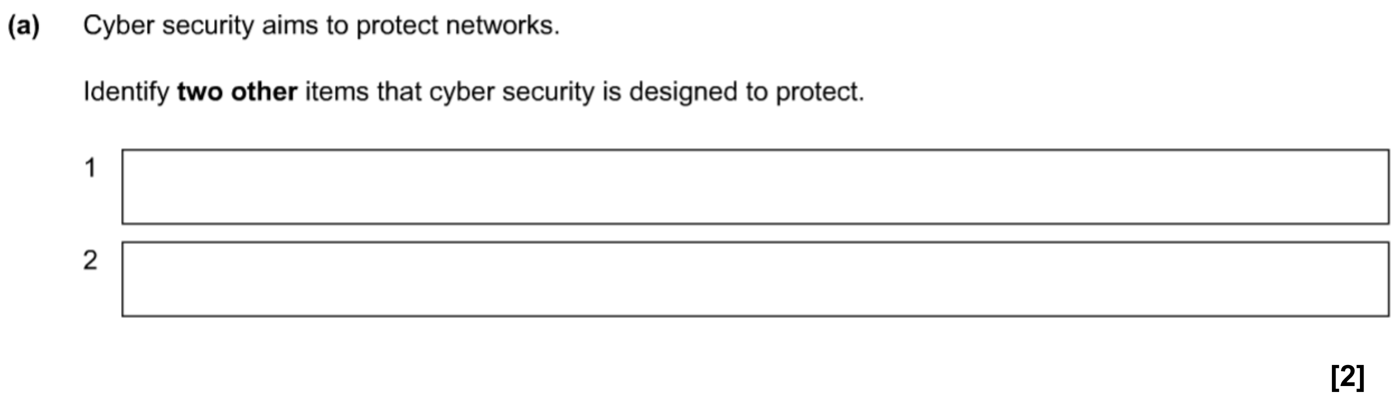
There are large numbers of candidates who are not attempting all questions and this is preventing them from accessing the higher grades.

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.

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 answers to the scenario in the question • Used the keywords in the question to give appropriate depth to their response.	• Missed questions out • Gave learnt responses from previous mark schemes that were not applicable • Used technical terms incorrectly.

Appendix 1 Questions

Question 1



(a) Cyber security aims to protect networks.

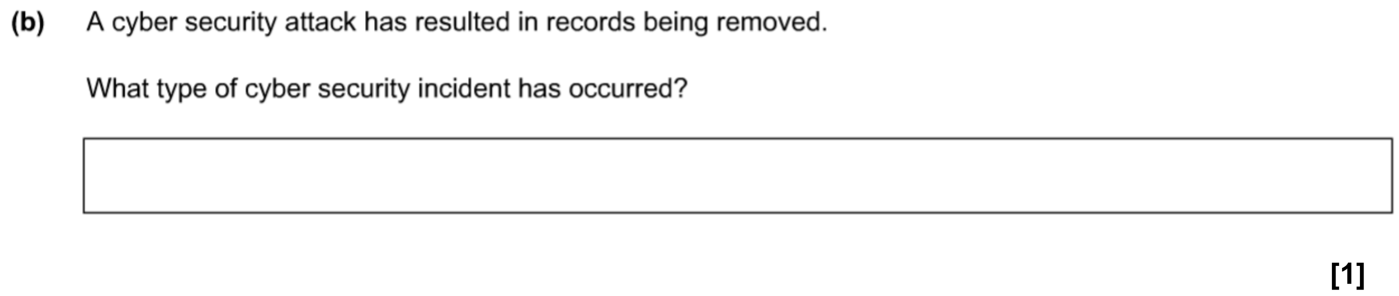
Identify **two other** items that cyber security is designed to protect.

1

2

[2]

This question was done reasonably well with candidates able to identify items that cyber security protects. Some candidates gave examples which allowed them to access the mark. Unfortunately, some did not read the question correctly and gave networks as a response.



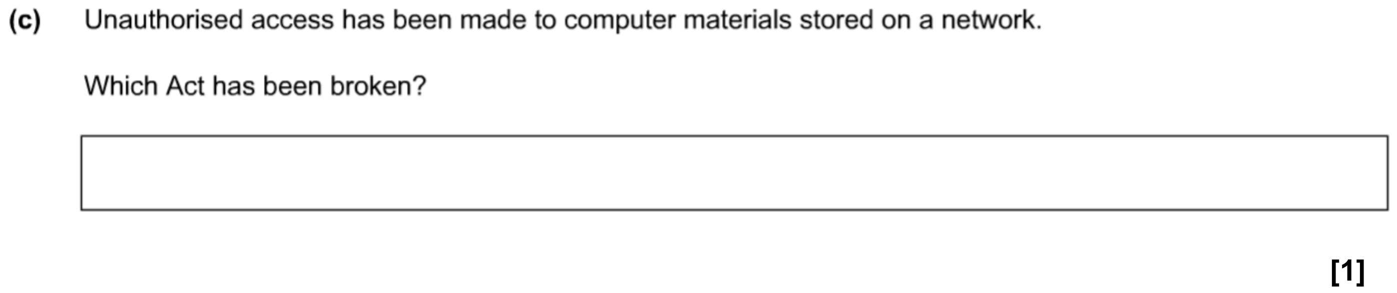
(b) A cyber security attack has resulted in records being removed.

What type of cyber security incident has occurred?

[1]

Many candidates correctly identified the type of incident.

?	**Misconception**	Data manipulation is altering the data not removing it.



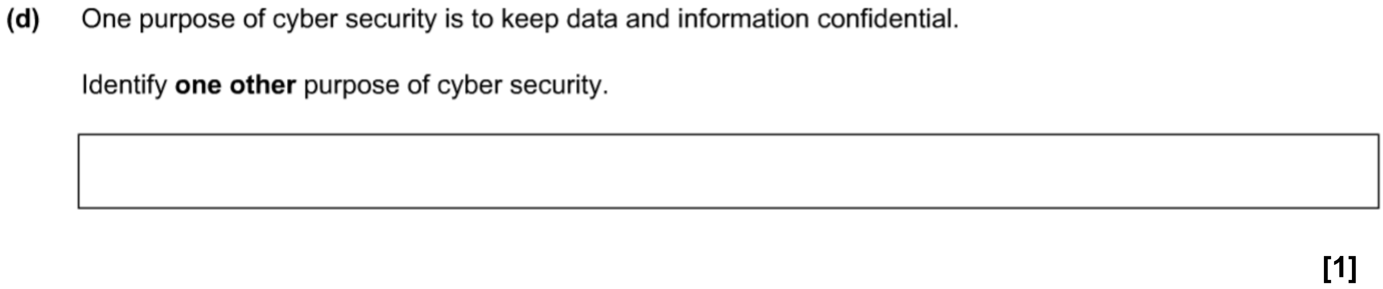
(c) Unauthorised access has been made to computer materials stored on a network.

Which Act has been broken?

[1]

There was very little understanding shown here with few candidates getting the answer correct.

?	**Misconception**	The Data Protection Act protects the data from misuse by the company, the Computer Misuse Act protects the data from external hackers.



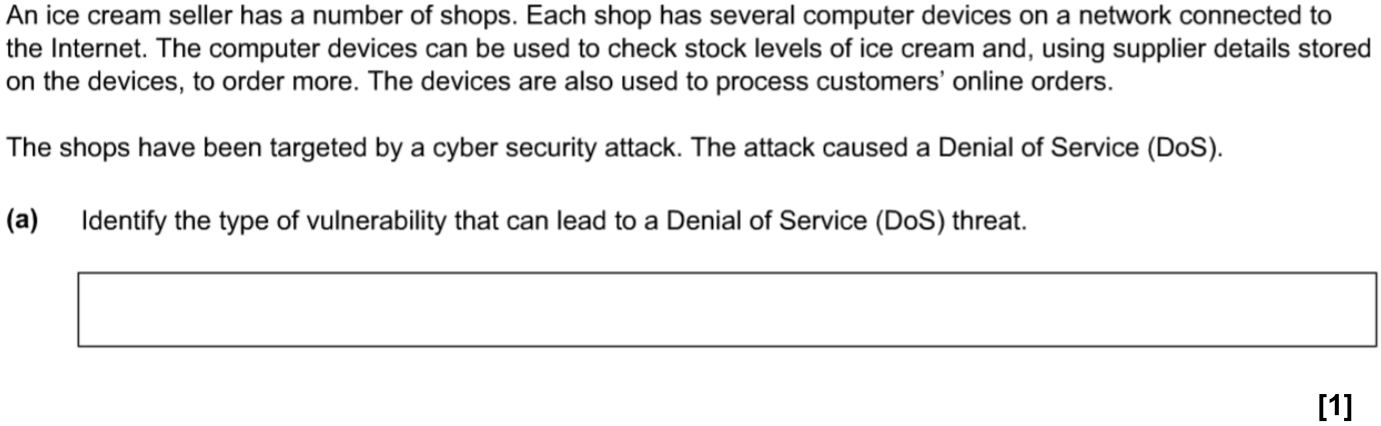
(d) One purpose of cyber security is to keep data and information confidential.

Identify **one other** purpose of cyber security.

[1]

This is a learn response on the purposes of cyber security. Many students reworded the example given in the question – confidentiality rather than give different ones.

Question 2



An ice cream seller has a number of shops. Each shop has several computer devices on a network connected to the Internet. The computer devices can be used to check stock levels of ice cream and, using supplier details stored on the devices, to order more. The devices are also used to process customers' online orders.

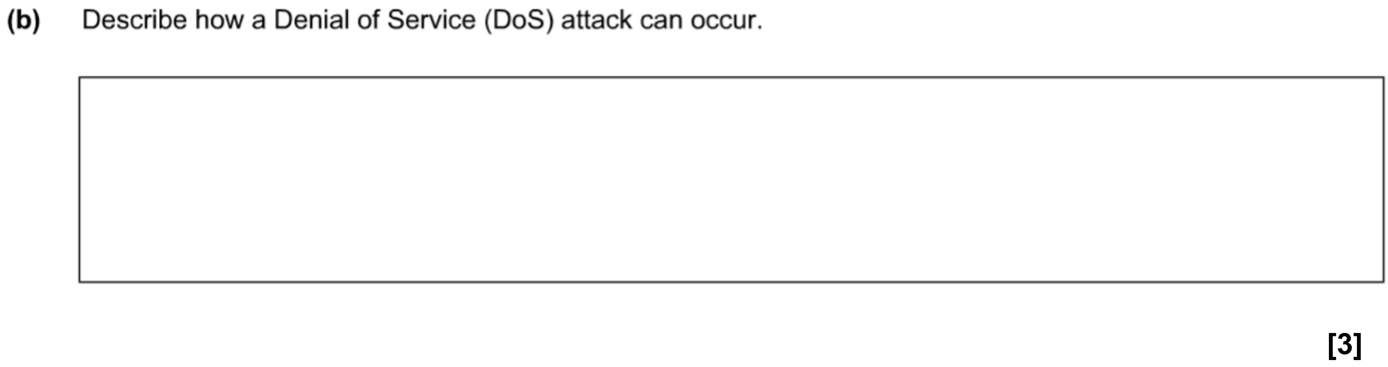
The shops have been targeted by a cyber security attack. The attack caused a Denial of Service (DoS).

(a) Identify the type of vulnerability that can lead to a Denial of Service (DoS) threat.

[1]

Many candidates gave responses based on what DoS and answered part (b).

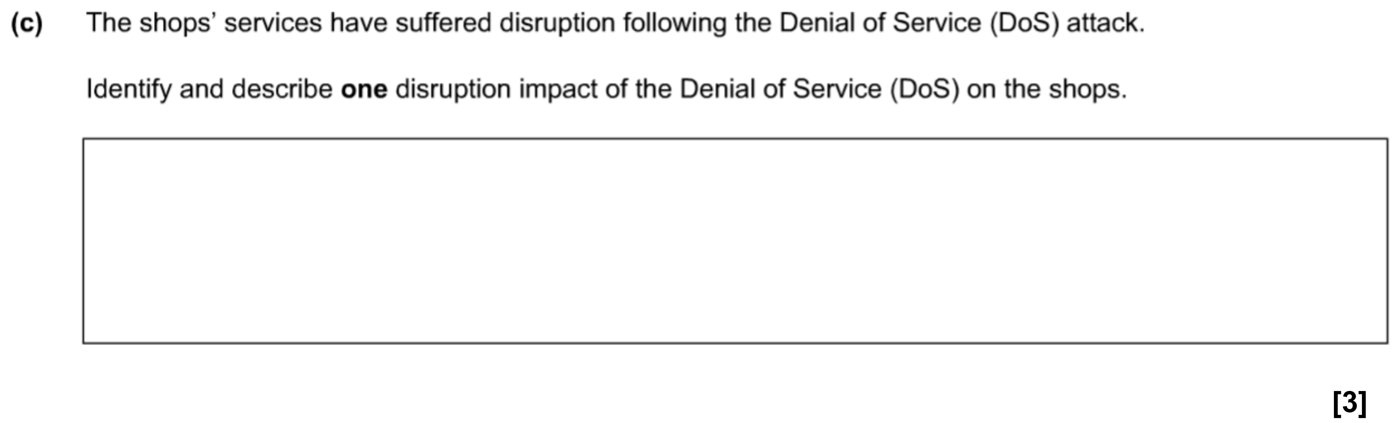
?	**Misconception**	There is a difference between how the vulnerability can be exploited and the type of vulnerability.



(b) Describe how a Denial of Service (DoS) attack can occur.

[3]

This question required a technical description based on the keyword "how". Very few candidates were aware of the specifics of an attack and gained few marks.



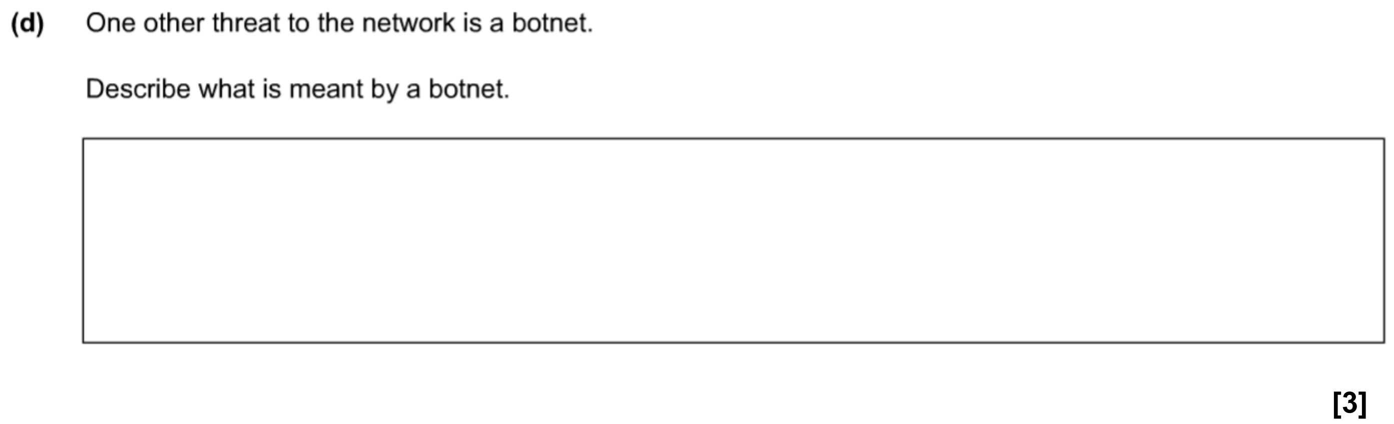
(c) The shops' services have suffered disruption following the Denial of Service (DoS) attack.

Identify and describe **one** disruption impact of the Denial of Service (DoS) on the shops.

[3]

The answer needed to be based on an impact that caused the day to day operation of the shops to be altered from their normal way of working. Many candidates referred to the inaccessibility of the website causing ordered not to be placed which gained marks.

↻	**AfL**	Where a question asks for an identification followed by a description, it is important that the candidate begins their response with a single word/phrase and then continues to expand on this.

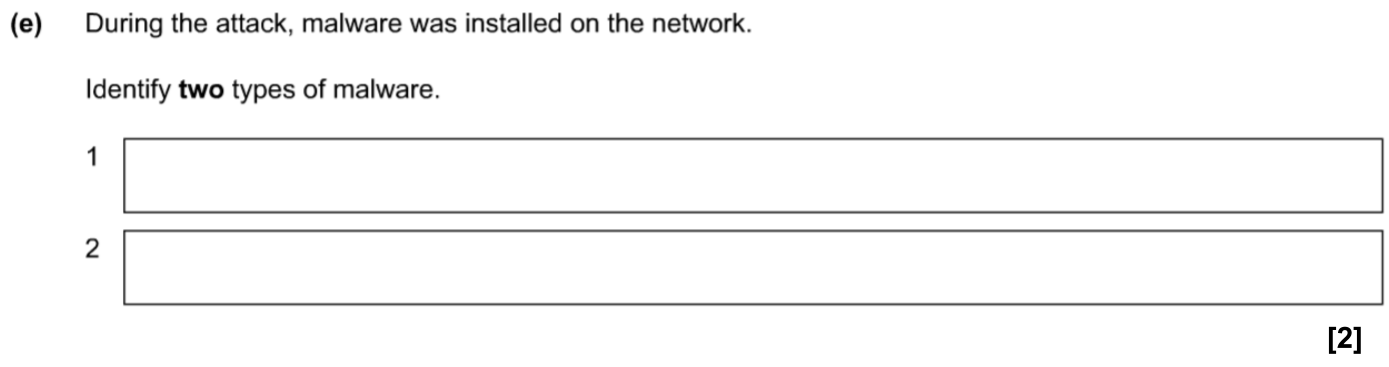


(d) One other threat to the network is a botnet.

Describe what is meant by a botnet.

[3]

There was much confusion regarding the description of a botnet and few marks were obtained by candidates.



(e) During the attack, malware was installed on the network.

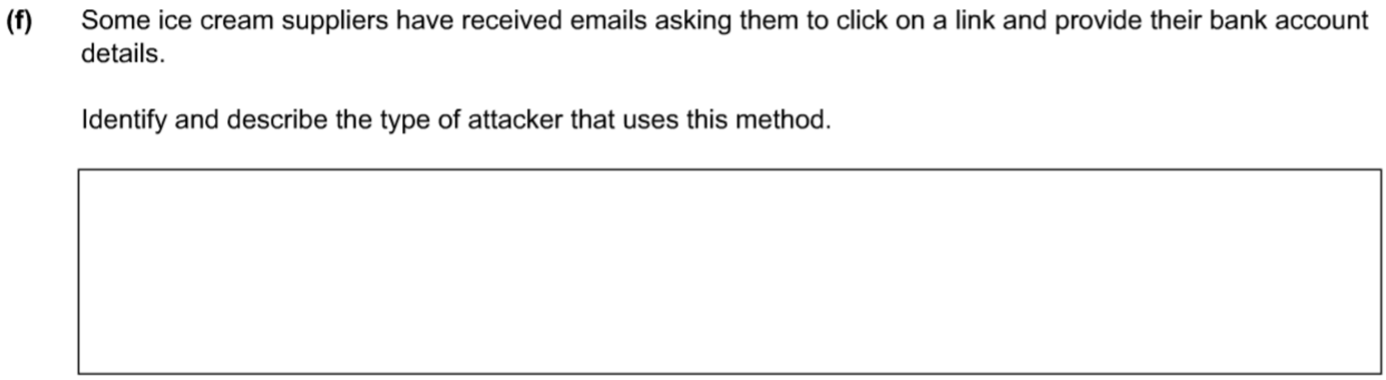
Identify **two** types of malware.

1

2

[2]

This was done very well with a large proportion of candidates identifying at least one type of malware with many obtaining both the marks available.



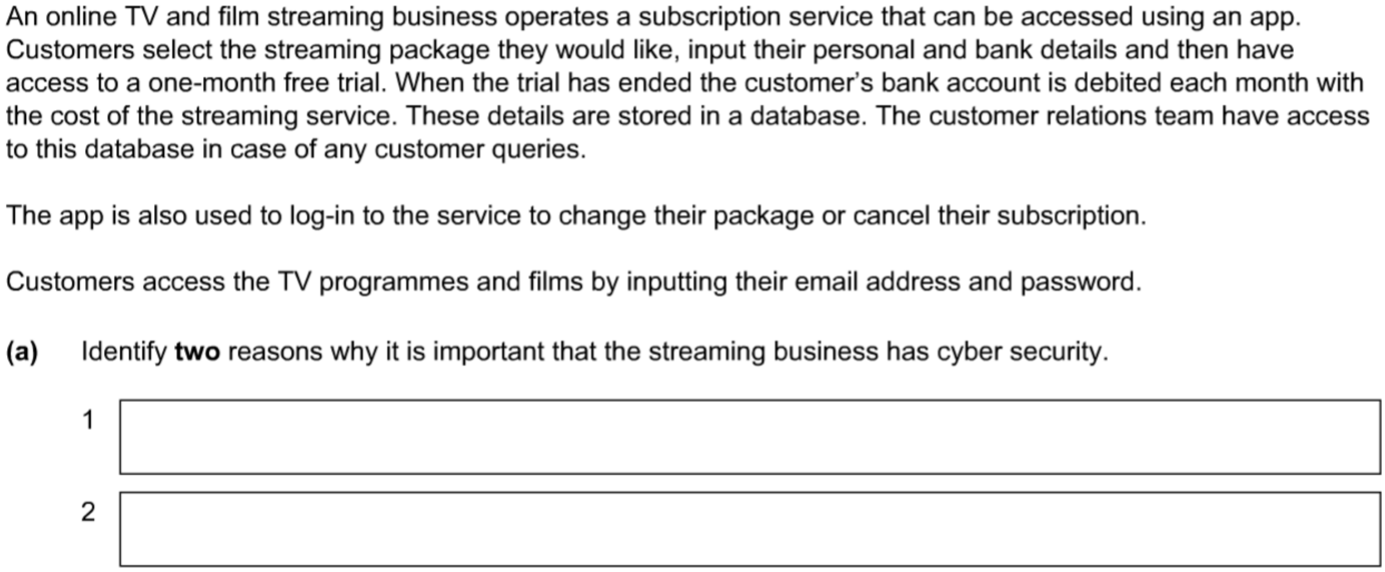
(f) Some ice cream suppliers have received emails asking them to click on a link and provide their bank account details.

Identify and describe the type of attacker that uses this method.

[3]

Candidates need to be aware of the different types of attacker and the methods that each type uses to gain access to secure systems. It was encouraging to see many candidates able to identify the attacker in the question as a phisher but the subsequent descriptions often lacked clarity and subsequent marks were not obtained.

Question 3



An online TV and film streaming business operates a subscription service that can be accessed using an app. Customers select the streaming package they would like, input their personal and bank details and then have access to a one-month free trial. When the trial has ended the customer's bank account is debited each month with the cost of the streaming service. These details are stored in a database. The customer relations team have access to this database in case of any customer queries.

The app is also used to log-in to the service to change their package or cancel their subscription.

Customers access the TV programmes and films by inputting their email address and password.

(a) Identify **two** reasons why it is important that the streaming business has cyber security.

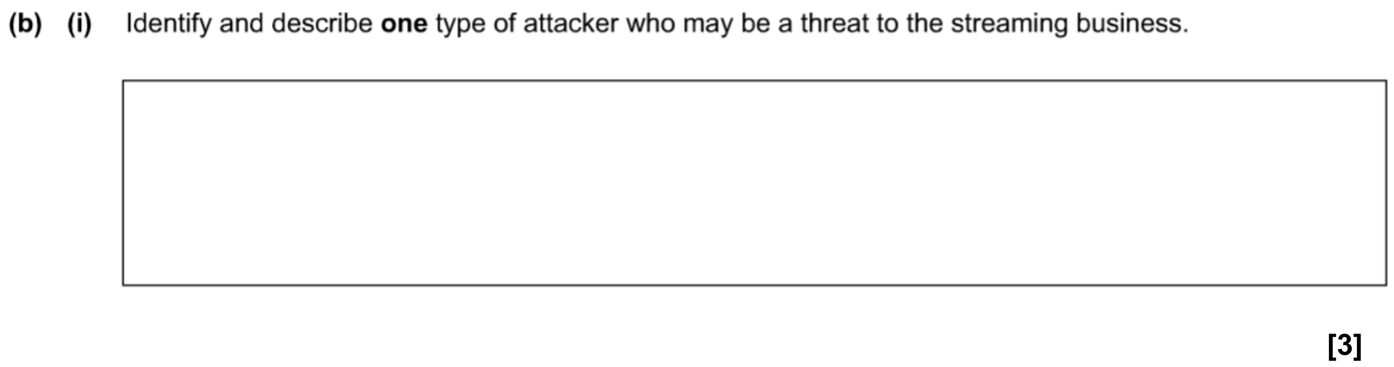
1

2

[2]

This question targets the basic need for cyber security and is something that all candidates should be aware of. A scenario is given in the stem of Question 3 and the candidate can use the information given to contextualise their reasons.

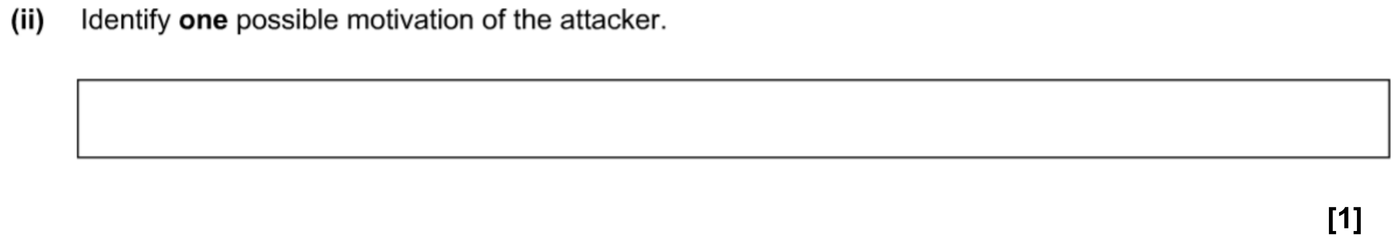
Very few candidates used the scenario in their responses; they were generic, regurgitated from previous mark schemes and did not secure marks.



(b) **(i)** Identify and describe **one** type of attacker who may be a threat to the streaming business.

[3]

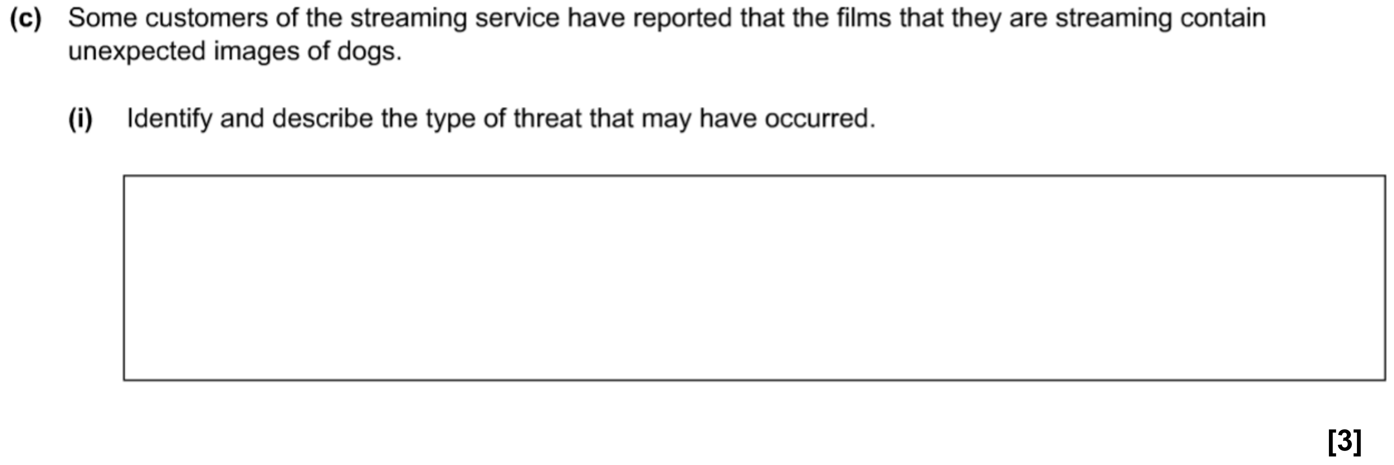
As with 2(f), knowing who the attacker is, is an important aspect of cyber security. The type of attacker needs to be identified before any marks can be gained from the description. The responses from many candidates included descriptions that were not specific to a type of attacker and contained no identification so could not be given marks.



(ii) Identify **one** possible motivation of the attacker.

[1]

This was very well done with the majority of candidates able to identify one reason why attacks take place.



(c) Some customers of the streaming service have reported that the films that they are streaming contain unexpected images of dogs.

(i) Identify and describe the type of threat that may have occurred.

[3]

The attacker accessed the video of the film and edited it. The question was asking what threat would have allowed this to happen. Very few candidates gave a threat that would allow the hacker access to the computer system. Many gave a description of different ways that the video could have been edited – the majority of which, while reasonable, did not obtain marks as they did not answer the question.

(ii) Identify and describe **one** logical prevention measure that could be used to stop this type of attack.

[3]

Without an understanding of the threat, it was difficult for candidates to gain marks for this question. The question asked for how the threat could be prevented and required a logical method. Both parts were required before marks could be given.

(iii) Explain how this threat to the streaming service could have been accidentally started.

[3]

Following on from the threat identification in the previous question, the focus here is on accidental. Many threats are intentional, but some are started by accident. The question here to trying to discern if the candidate was aware of the difference. The question required an understanding of the threat, the measure used to prevent the threat and how the threat could have originally been started. The set of Questions (i), (ii) and (iii) move the scenario through the life of the attack. Many students did not relate the three parts of the question together but answered them independently of each other.

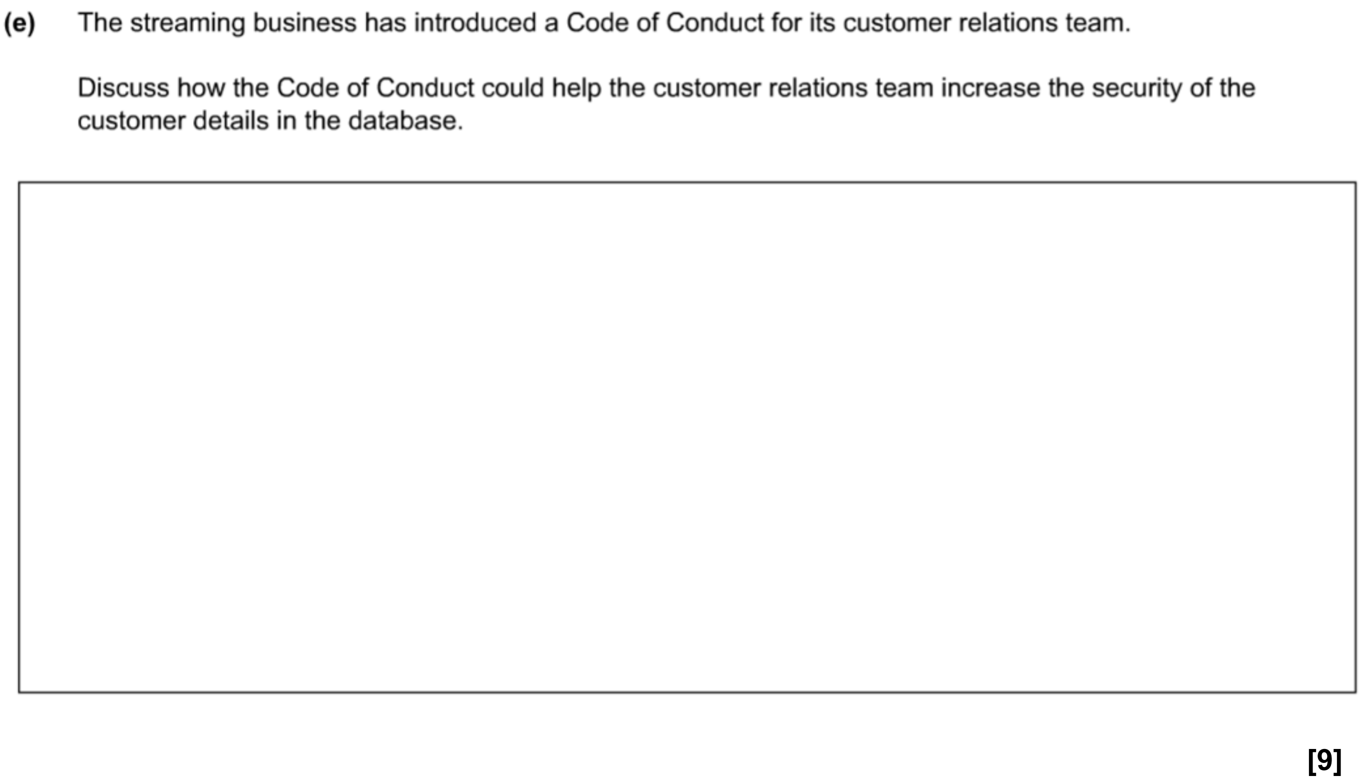
	AfL	Any question that is based around sub parts are linked together and need to be read through first before starting on the first part.

(d) Following the attack, some customers reported that their email address was no longer recognised.

Identify the type of cyber security incident that may have occurred.

[1]

The question indicated that the email address stored was different from the one being entered by the customer and asked for the type of incident that could have caused this. The answer was based on the stored data being deleted or altered. Many responses were based on identity theft – this would not have resulted in changed or deleted data. It is important that the candidate reads the context and scenario carefully before forming their response.



(e) The streaming business has introduced a Code of Conduct for its customer relations team.

Discuss how the Code of Conduct could help the customer relations team increase the security of the customer details in the database.

[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 the customer relations team – they are an internal part of the company and how codes of conduct can increase security. A significant proportion of candidates answered it from the customer and what they could do to protect their data without any reference to codes of conduct. From those that did identify valid points, few went on to discuss how security could be increased, instead making a series of single points.

⟳	**AfL**	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.

Copyright

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

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 2020-2021

Our priority is supporting you and your students as you prepare for summer 2021 exams. We'll update our website information regularly with resources, guidance and key information.

Take a look at our support for:

- Teachers
- Students
- Exams officers
- Assessment specialists

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 2020-2021 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.

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.

General qualifications
01223 553998
general.qualifications@ocr.org.uk

Vocational qualifications
02476 851509
vocational.qualifications@ocr.org.uk

For more information visit
ocr.org.uk/i-want-to/find-resources/
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**

Cambridge Assessment