PrepWithTee

NOTES

The Internet and its Uses

Cambridge O Level Computer Science (2210)

The full notes for this chapter: the topic taught from the basics, then how it is examined - question types, marking points, keywords and real past-paper questions solved - with practice to finish.

Contents

1	The internet, the web and browsers	8 min
2	Locating web pages and cookies	9 min
3	Digital currency and blockchain	5 min
4	Cyber security threats	10 min
5	Keeping data safe	8 min

Each note has two parts. **Part 1** teaches the topic from the basics. **Part 2** shows how it is examined: the types of question, what the examiner gives marks for, the keywords to use, and real past-paper questions solved with the official mark scheme. The answers to every practice question are at the end of each note.

NOTE 1

The internet, the web and browsers

1 In this note

SYLLABUS 5.1 THE INTERNET AND THE WORLD WIDE WEB

- 5.1.1 Understand the difference between the **internet** and the **world wide web**.
- 5.1.2 Understand what is meant by a **uniform resource locator (URL)**.
- 5.1.3 Describe the purpose and operation of **HTTP** and **HTTPS**.
- 5.1.4 Explain the purpose and functions of a **web browser**.

Next: Locating web pages and cookies.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

IP addresses

Every device on the internet is identified by an IP address.

Quick check: who allocates a device's IP address?

The network (the router).

Asymmetric encryption

Data encrypted with a public key can only be decrypted with the matching private key.

Quick check: who holds the private key?

Only its owner (e.g. the web server).

3 The internet and the world wide web

The internet	The world wide web (WWW)
the **infrastructure**: a global network of interconnected networks (cables, routers, servers)	the **collection of websites and web pages** that are **accessed using the internet**
carries many services: email, video calls, online games, file transfer … and the web	is just one of the services that uses the internet

> Think of the internet as the **roads** and the world wide web as the **shops** you reach by using them.

4 URLs

A **uniform resource locator (URL)** is a **text-based address** for a web page. It is easier for people to remember than an IP address. A URL can contain the **protocol**, the **domain name** and the **web page / file name**.



The parts of the URL https://www.examplebooks.com/maths/index.html.

5 HTTP and HTTPS

A **protocol** is a set of rules for transmitting data. **Hypertext transfer protocol (HTTP)** is the protocol used to **request and send web pages** between a web browser and a web server. **HTTPS** (hypertext transfer protocol secure) is HTTP with security added: it uses **SSL / TLS** to **encrypt** the data, so if it is intercepted it cannot be understood. Websites that take passwords or payments should use HTTPS (the padlock in the address bar).

GENERAL METHOD **How HTTPS / SSL secures the connection**

1. The **web browser** asks the **web server** to identify itself.
2. The web server sends back its **digital certificate** (which contains its **public key**).
3. The web browser **authenticates** the certificate (checks it is genuine and in date).
4. If it is authentic, **encrypted** data transmission begins: data is encrypted with the server's public key, and only the server's **private key** can decrypt it.

6 Web browsers

A **web browser** is the software used to access and view web pages. Its **main purpose** is to **render HTML and display web pages**. (**HTML**, hypertext markup language, is the language web pages are written in, with tags such as <head> and <body>.)

Function	Example
storing bookmarks and favourites	jump straight to a site you visit often
recording user history	find a page you visited yesterday
allowing **multiple tabs**	have several web pages open at once
storing cookies	stay logged in; payment details filled in for you
providing **navigation tools**	back, forward, refresh, home buttons
providing an **address bar**	type in a URL

TRY IT YOURSELF

1. Which is the infrastructure: the internet or the world wide web?
2. In https://www.examplebooks.com/maths/index.html, what is the domain name?
3. Which browser function lets you return quickly to a site you use often?

7 Summary

- Internet = infrastructure (network of networks). WWW = collection of web pages accessed using the internet.
- URL = text-based address: protocol + domain name + web page / file name.
- HTTP: protocol to request and send web pages. HTTPS: HTTP + SSL/TLS encryption, digital certificate.
- Browser: main purpose = render HTML and display web pages; bookmarks, history, tabs, cookies, navigation, address bar.

IF YOU SEE …

"describe the difference between the internet and the WWW"	→ infrastructure … whereas … collection of web pages
"explain how HTTPS makes transmission secure"	→ SSL/TLS · encrypts · meaningless if intercepted · public / private key · certificate

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

8 Ways they test it

TYPE 1 **Internet vs WWW**

> *"Describe the difference between the internet and the world wide web" [2]*

Spot it "difference".

1 Two facts, joined by "whereas".

TYPE 2 **URL parts**

> *"Identify the three different parts of the URL" [3]; a labelled URL*

Spot it a URL.

1. protocol · domain name · file (web page) name

TYPE 3 **Browser**

> *"Explain the purpose of the web browser" [2]; "give three other functions" [3]; "which function ..." [1]*

Spot it "browser".

1. Purpose: renders HTML, displays web pages. Functions from the table.

TYPE 4 **SSL paragraph**

> *"The ... asks the ... to identify itself ..." [5]*

Spot it a word list.

1. Follow the HTTPS method.

9 What the examiner looks for

"Explain how HTTPS makes the transmission of data secure" [4]

Marking points (one mark each, up to the marks shown)

- Uses SSL / TLS
- Encrypts the data ...
- ... which stops the data being understood if it is intercepted
- ... using asymmetric encryption: data encrypted with the web server's public key
- ... can only be decrypted with the web server's private key

KEYWORDS **SSL** **encrypts** **intercepted** **public key** **private key**

10 Past-paper questions, solved

2210/12/M/J/24 Q11 ↗ Paper 1 · Computer systems **8 marks** ⤢ Full size

11 A company has a website. Users use the internet and the world wide web to access the website.

(a) Describe the difference between the internet and the world wide web.

..... [2]

(b) The website has a uniform resource locator (URL). The URL has three different parts.

Identify the **three** different parts that are included in the URL.

[3]

(c) One function of a web browser is to provide an address bar for a user to enter a URL.

Give **three** other functions of a web browser.

[3]

Swipe sideways to read the whole question

How to start (c) the address bar is given, so pick three other functions.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) The internet is the infrastructure, whereas the world wide web is the collection of web pages accessed using it.

(b) Protocol; domain name; web page (file) name.

(c) Storing bookmarks and favourites; recording the user's history; allowing multiple tabs.

PART	ANSWER / WORKING	MARKS	GUIDANCE
11(a)	internet is the infrastructure · WWW is a collection of web pages	B2	
11(b)	protocol · domain name · file name // web page name	B3	
11(c)	Any three: displays web pages · bookmarks · history · tabs · cookies · navigation tools · home page	B3	

Total: 8 marks

2210/12/O/N/24 Q7 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

7 A student enters the uniform resource locator (URL) for a web page into their tablet computer.

(e) The data for the web page is transmitted using the secure socket layer (SSL) protocol.

Complete the paragraph about the SSL protocol.

Use only terms from the list.

Not all terms need to be used. Some terms may be used more than once.

encrypted file server hypertext markup language (HTML)

hypertext transfer protocol (HTTP) operating system search engine

unencrypted URL web browser web server

The ..... asks the .....

to identify itself. The ..... sends back its digital

certificate. The ..... authenticates the digital certificate.

If it is authentic, ... data transmission begins.

[5]

Swipe sideways to read the whole question

How to start Follow the HTTPS method: who asks, who answers, who checks.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

The **web browser** asks the **web server** to identify itself. The **web server** sends back its digital certificate. The **web browser** authenticates the digital certificate. If it is authentic, **encrypted** data transmission begins.

PART	ANSWER / WORKING	MARKS	GUIDANCE
7(e)	web browser · web server · web server · web browser · encrypted	B5	

Total: 5 marks

4 An employee uses a web browser on their computer.

(a) Describe the main purpose of a web browser.

..... [2]

(b) The employee wants his payment details to be automatically filled in when he buys products using the internet.

Identify the function of a web browser that could be used for this purpose.

..... [1]

(c) The employee wants to be able to quickly access websites that he regularly uses.

Identify the function of a web browser that could be used for this purpose.

..... [1]

(d) The web browser uses the secure socket layer (SSL) protocol to transmit personal data securely over the internet.

State how the SSL protocol secures the data for transmission.

..... [1]

Swipe sideways to read the whole question

How to start (b) and (c) each name ONE browser function from the table.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) To display web pages, by rendering HTML.

(b) Storing cookies.

(c) Storing bookmarks / favourites.

(d) It encrypts the data.

PART	ANSWER / WORKING	MARKS	GUIDANCE
4(a)	display web pages · by rendering HTML	B2	
4(b)	storing cookies	B1	
4(c)	bookmarks // favourites	B1	
4(d)	encrypts it // uses digital certificates	B1	
		Total: 5 marks	

11 Common mistakes

✗ "The internet and the WWW are the same" ✓ "The internet is the infrastructure; the WWW is the web pages"

✗ "A browser finds the IP address" ✓ "The DNS finds the IP address; the browser renders HTML"

Next note.

✗ "HTTPS is faster" ✓ "HTTPS encrypts the data (SSL/TLS)"

12 Practice

Practice: easy, medium, hard

1. What does URL stand for?
2. What does the S in HTTPS stand for?
3. Which language are web pages written in?
1. State the main purpose of a web browser.
2. Give two functions of a web browser other than an address bar.
1. Explain why an online shop should use HTTPS. [2]

13 Can I do this?

0 / 4 ticked

- [ ] I can explain the difference between the internet and the WWW.
- [ ] I can name the parts of a URL.
- [ ] I can describe HTTP and how HTTPS secures data.
- [ ] I can give the purpose and functions of a web browser.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER The internet

2.

ANSWER www.examplebooks.com

3.

ANSWER Bookmarks / favourites

Practice: easy, medium, hard

Easy 1.

ANSWER Uniform resource locator

Easy 2.

ANSWER Secure

Easy 3.

ANSWER HTML

Medium 1.

ANSWER To render HTML and display web pages

Medium 2.

ANSWER e.g. bookmarks, history (also tabs, cookies, navigation tools)

Hard 1.

ANSWER

Customers enter personal / payment details; HTTPS encrypts them so they are meaningless if intercepted

NOTE 2

Locating web pages and cookies

1 In this note

SYLLABUS 5.1 THE INTERNET AND THE WORLD WIDE WEB

- 5.1.5 Describe how web pages are **located, retrieved and displayed** when a user enters a URL: the role of the **web browser**, **IP addresses**, the **domain name server (DNS)**, the **web server** and **HTML**.
- 5.1.6 Explain what is meant by **cookies** and how they are used, including **session** and **persistent** cookies.

Before this: The internet, the web and browsers. Next: Digital currency and blockchain.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

URLs and IP addresses

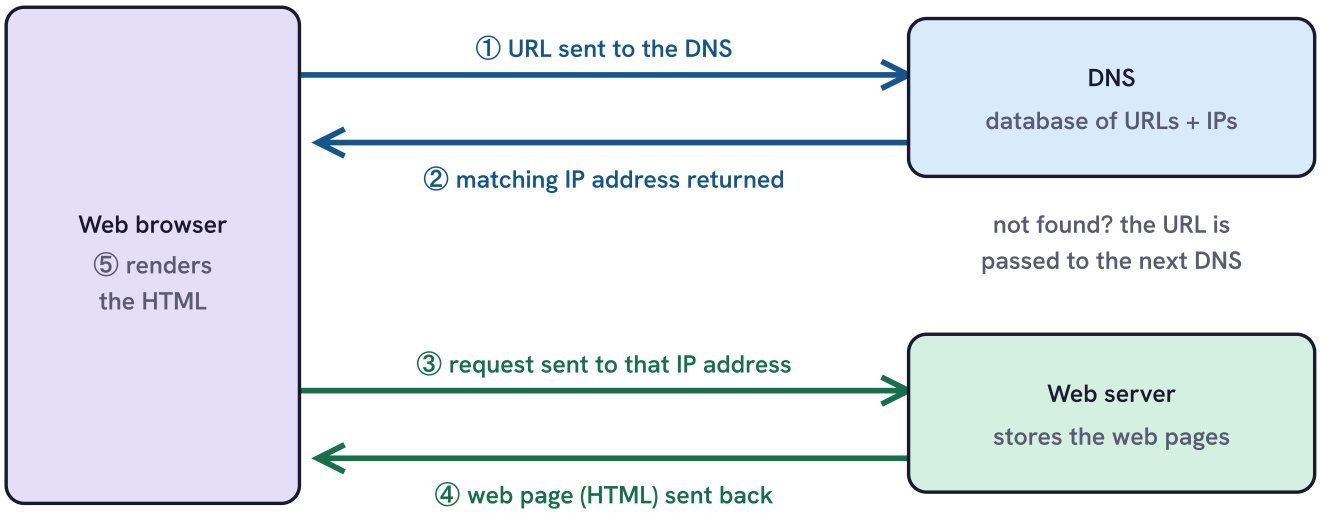
People type URLs; computers find each other by IP address.

Quick check: what has to happen before the browser can contact the web server?

The URL must be turned into the server's IP address.

3 From URL to web page

A **domain name server (DNS)** is a server that stores a **database of URLs (domain names) and their matching IP addresses**. A **web server** is a server that **stores web pages** and sends them to clients that request them.



The five steps, ① to ⑤.

GENERAL METHOD **How a web page is located, retrieved and displayed**

1. The user enters the **URL** into the **address bar** of the **web browser**.
2. The browser sends the URL to a **DNS**.
3. The DNS **searches its database** for the matching **IP address**. If it cannot find it, the URL is **sent to the next DNS** until it is found.
4. The DNS **returns the IP address** to the web browser.
5. The browser sends a **request** to the **web server** at that IP address.
6. The web server sends the web page data, the **HTML** files, back to the browser.
7. The browser **renders the HTML** and **displays** the web page.

4 Cookies

A **cookie** is a **small text file** that is sent between a **web server** and a **web browser** and **stored by the browser**. It lets a website remember information about the user.

Session cookie	Persistent cookie
temporary: stored in **memory (RAM)**, not in secondary storage	**permanent**: stored on the user's **secondary storage**
deleted when the browser is closed	**kept** when the browser is closed, until it **expires** or the user **deletes** it
e.g. holding items in a shopping cart during one visit	e.g. staying logged in; remembering preferences for next time

Uses of cookies	
saving personal details	name, address filled in for you
tracking user preferences	language, dark mode, items you looked at (targeted adverts)
holding items in an online shopping cart	the basket keeps its contents as you browse
storing login details	you stay logged in

TRY IT YOURSELF

1. Which server stores a database of URLs and IP addresses?
2. Which type of cookie is deleted when the browser is closed?
3. What does the browser receive from the web server to display the page?

5 Summary

- URL → DNS → IP address back → request to the web server's IP → HTML back → browser renders it.
- If a DNS can't find the URL, it passes it to another DNS.
- Cookie: small text file, sent between server and browser, stored by the browser.
- Session: in RAM, lost when the browser closes. Persistent: on secondary storage, until it expires / is deleted.
- Uses: personal details, preferences, shopping cart, login details.

IF YOU SEE …

"describe how the web pages are located, retrieved and displayed" [6]	→ browser · URL to DNS · IP returned · request to web server · HTML sent · rendered
"explain the difference between session and persistent cookies"	→ RAM … whereas secondary storage · lost on close … whereas kept until expiry

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

6 Ways they test it

TYPE 1 **Describe / draw**

> *"Draw and annotate a diagram to show the process from entering the URL to displaying the page" [5]; "describe how the web pages are located, retrieved and displayed" [6]*

Spot it "located", "diagram".

1. Boxes: browser, DNS, web server. Number the arrows and say what travels along each.

TYPE 2 **Role of the DNS**

> *"Describe the role of the DNS" [2]*

Spot it "DNS".

1. database of URLs + IPs · finds the IP · next DNS · returns it

TYPE 3 **Cookie cloze**

> *"Cookies are small … files that are sent between a … and a …" [6-7]*

Spot it a word list.

1. Use the two tables.

TYPE 4 **Cookie uses / difference**

> *"Give three functions of a cookie" [3]; "explain the difference between session and persistent cookies" [4]*

Spot it "cookie".

1. Comparisons need both sides.

7 What the examiner looks for

Diagram from entering the URL to displaying the page [5]

Marking points (one mark each, up to the marks shown)

- URL sent from the browser to the DNS
- DNS stores a database of URLs and IPs // finds the IP for the URL
- If not found, sent to the next / a higher DNS
- DNS sends the IP address to the browser
- Browser sends a request to the IP address of the web server
- Web server processes the request; web page (HTML) data sent to the browser
- Browser renders the HTML

KEYWORDS **DNS** **IP address** **web server** **request** **HTML** **render**

8 Past-paper questions, solved

2210/12/M/J/23 Q6 ↗ Paper 1 · Computer systems **9 marks** ⤢ Full size

6 (a) Complete the statements about cookies.

Use the terms from the list.

Some of the terms in the list will **not** be used. Some terms may be used more than once.

compression	executable	hypertext markup language (HTML)
hypertext transfer protocol (HTTP)	image	internet protocol (IP) address
persistent	session	sound
text		
uniform resource locater (URL)	web browser	web server

Cookies are small ..... files that are sent between a ..... and a ..... .

..... cookies are stored in memory and **not** in the user's secondary storage.

When the web browser is closed a ..... cookie is lost, whereas a ..... cookie is **not** lost.

[6]

(b) Give **three** functions of a cookie.

1 .....

2 .....

3 .....

[3]

Swipe sideways to read the whole question

How to start Session = memory, lost when closed; persistent = kept.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) Cookies are small **text** files that are sent between a **web browser** and a **web server**. **Session** cookies are stored in memory and not in the user's secondary storage. When the web browser is closed a **session** cookie is lost, whereas a **persistent** cookie is not lost.

(b) Saving personal details; storing login details; holding items in an online shopping cart.

PART	ANSWER / WORKING	MARKS	GUIDANCE
6(a)	text · web browser · web server (either order) · session · session · persistent	B6	
6(b)	Any three: personal details · login details · user preferences · shopping cart	B3	

Total: 9 marks

0478/13/M/J/24 Q7 ↗ Paper 1 · Computer systems — **6 marks** — ⤢ Full size

7 A company has a network that includes a web server.

Data is transmitted across the network using serial half-duplex data transmission.

(e) Customers access the company's web pages that are stored on the web server.

Describe how the web pages are located, retrieved and displayed on a customer's computer.

..... [6]

Swipe sideways to read the whole question

How to start Six marks: follow the seven-step method from the browser to the rendered page.

▾ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

The customer types the URL into the web browser, which sends it to a DNS. The DNS searches its database for the matching IP address (passing the URL to another DNS if it cannot find it) and returns the IP address to the browser. The browser sends a request to the web server at that IP address. The web server sends the HTML for the web page back, and the browser renders the HTML to display the page.

PART	ANSWER / WORKING	MARKS	GUIDANCE
7(e)	Any six: URL into browser · sent to DNS · DNS finds matching IP · next DNS if not found · IP returned · request to web server · HTML sent back · browser renders HTML	B6	

Total: 6 marks

2210/11/M/J/23 Q10 ↗ Paper 1 · Computer systems — **4 marks** — ⤢ Full size

10 A student uses the internet for their schoolwork to research what is meant by pharming.

(e) A student visits a website that uses session cookies, instead of persistent cookies.

Explain the difference between session cookies and persistent cookies.

..... [4]

Swipe sideways to read the whole question

How to start Four marks: two differences, each stated for both types.

▾ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

Session cookies are stored in memory (RAM), whereas persistent cookies are stored on secondary storage. When the browser is closed a session cookie is lost, whereas a persistent cookie is kept until it expires or the user deletes it.

PART	ANSWER / WORKING	MARKS	GUIDANCE
10(e)	Any four: session in RAM … persistent on secondary storage · session lost when browser closed … persistent not lost … until deleted / expires	**B4**	

Total: 4 marks

9 Common mistakes

✗ "The DNS sends the web page"	✓ "The DNS sends the IP address; the web server sends the web page"
✗ "Cookies are programs / viruses"	✓ "Cookies are small text files"
✗ "Session cookies are stored on the hard drive"	✓ "Session cookies are stored in RAM"

10 Practice

Practice: easy, medium, hard

1. Which server stores the web pages?
2. Where is a persistent cookie stored?

1 Describe the role of the DNS. [2]

2 Give two uses of cookies.

1 A user closes the browser with items in their basket. When they return the items are gone. Which type of cookie was used? Explain. [2]

11 Can I do this?

0 / 2 ticked

- [ ] I can describe how a web page is located, retrieved and displayed.
- [ ] I can explain cookies, session vs persistent, and their uses.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER DNS (domain name server)

2.

ANSWER Session cookie

3.

ANSWER HTML (the web page data)

Practice: easy, medium, hard

Easy 1.

ANSWER Web server

Easy 2.

ANSWER Secondary storage

Medium 1.

ANSWER

Stores a database of URLs and matching IP addresses; finds the IP for a URL and returns it to the browser

Medium 2.

ANSWER e.g. storing login details; holding items in a shopping cart

Hard 1.

ANSWER Session cookie: stored in RAM and deleted when the browser was closed

NOTE 3

Digital currency and blockchain

1 In this note

SYLLABUS 5.2 DIGITAL CURRENCY

- 5.2.1 Understand the concept of a **digital currency** and how digital currencies are used.
- 5.2.2 Understand the process of **blockchain** and how it is used to **track digital currency transactions**.

Before this: Locating web pages and cookies. Next: Cyber security threats.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Encryption

Encryption scrambles data so that only someone with the key can read it.

Quick check: why encrypt a payment?

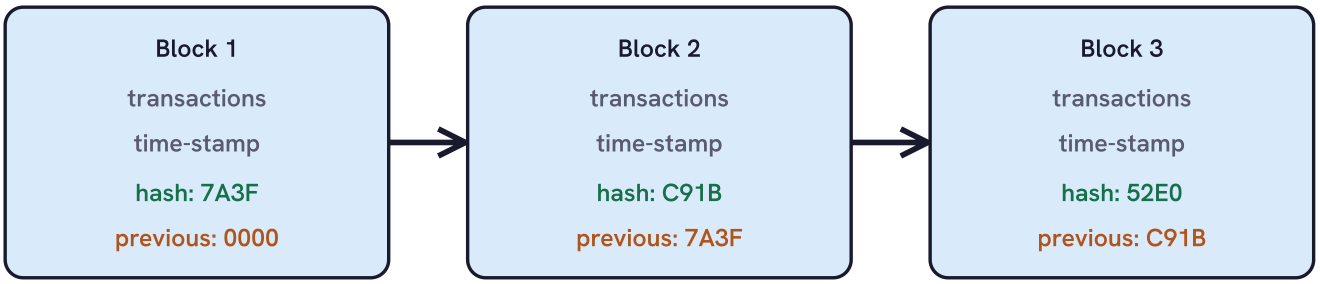
So it is meaningless if intercepted.

3 Digital currency

A **digital currency** is money that **only exists electronically**: there are no coins or notes. It can be used to pay for goods and services online and to transfer value between people. Some digital currencies are **centralised** (controlled by one organisation, like a bank), others are **decentralised** (no single organisation controls them; cryptocurrencies such as Bitcoin). Transactions are usually **encrypted**.

4 Blockchain

A **blockchain**, in its basic form, is a **digital ledger**: a **time-stamped series of records that cannot be altered**. Each new transaction is added to a **block**; each block is **linked to the previous block**, forming a chain. A copy of the chain is kept on many computers, so there is no single place to attack.



Changing block 1 would change its hash, so block 2 would no longer match: the change is detected.

Each block stores the hash of the block before it.

GENERAL METHOD

How a digital currency payment is tracked by blockchain

1. The payer's device **encrypts** the payment data and sends it to the **digital ledger**.
2. The transaction is recorded with a **time-stamp** (and a digital signature) and stored in a **block** with other transactions.
3. Each block has its own **hash** (unique identifier) and stores the **hash of the previous block**.
4. When the block is full it is **added to the blockchain** on **every computer** that holds a copy.
5. Records **cannot be altered**, only new ones added, so every transaction can be **traced**.

TRY IT YOURSELF

1. Does a digital currency exist physically?
2. What is the name of the process that uses a digital ledger to track digital currency?

3 What does each block store that links it to the chain?

5 Summary

- Digital currency: only exists electronically; may be centralised or decentralised; usually encrypted.
- Blockchain: a digital ledger, a time-stamped series of records that cannot be altered.
- Blocks of transactions, each with its own hash and the previous block's hash; copies on many computers.

IF YOU SEE …

"draw and annotate a diagram to show a payment using digital currency and blockchain" [4]	→ device encrypts · sent to ledger · recorded with time-stamp · stored in a block · block hash · added to the chain on every device

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

6 Ways they test it

TYPE 1 **Features**

> *"Give two other features of digital currency" [2]; "identify the process that uses a digital ledger" [1]*

Spot it "digital currency".

1 only electronic · centralised / decentralised · encrypted; blockchain

TYPE 2 **Cloze**

> *"A digital currency does not exist ..., ... digital ledgers called ..." [4]*

Spot it a word list.

1. physically · blockchains · time-stamp · traced

TYPE 3 **Diagram**

> *"Draw and annotate a diagram to show how a payment is made using digital currency and blockchain" [4]*

Spot it "diagram".

1. Follow the method; label the block hash.

7 Past-paper questions, solved

0478/12/F/M/24 Q5 ↗ Paper 1 · Computer systems — **4 marks** — ⤢ Full size

5 Complete the description of digital currencies using the terms provided.

blockchains changed datachains decentralised
deleted encryption passport physical address
physically records time-stamp traced
transaction-chains virtually

A digital currency does **not** exist ....., it can only be accessed electronically.

Some digital currencies have digital ledgers called ..... . These are decentralised databases where each transaction is stored as a new set of data with a ..... and is linked to the previous set of data. This means that transactions cannot be altered, only new transactions added, which allows the location of the data to be ..... .

[4]

Swipe sideways to read the whole question

How to start Four gaps: one from each line of the definition.

▾ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

A digital currency does not exist **physically**, it can only be accessed electronically. Some digital currencies have digital ledgers called **blockchains**. These are decentralised databases where each transaction is stored as a new set of data with a **time-stamp** and is linked to the previous set of data. This means that transactions cannot be altered, only new transactions added, which allows the location of the data to be **traced**.

PART	ANSWER / WORKING	MARKS	GUIDANCE
5	physically · blockchains · time-stamp · traced	B4	

Total: 4 marks

2210/12/O/N/23 Q12 ↗ Paper 1 · Computer systems **3 marks** ⤢ Full size

12 Digital currency can be used to pay for products and services.

Digital currencies are often tracked using digital ledgers.

(a) Give **two** other features of digital currency.

[2]

(b) Identify the process that uses a digital ledger to track the use of digital currency.

..... [1]

Swipe sideways to read the whole question

How to start The question already says digital ledger, so choose two other features.

▾ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) It only exists electronically; it is usually encrypted.

(b) Blockchain.

PART	ANSWER / WORKING	MARKS	GUIDANCE
12(a)	Any two: only exists electronically · decentralised · centralised · usually encrypted	B2	
12(b)	Blockchain	B1	

Total: 3 marks

8 Common mistakes

✗ "Records in a blockchain can be edited"

✓ "Records cannot be altered, only added"

✗ "Digital currency is money in a bank account"

Bank balances back real notes.

✓ "Digital currency only exists electronically"

9 Practice

Practice: easy, medium, hard

1. Give one example of a decentralised digital currency.
1. Explain why a blockchain is hard to tamper with. [2]
1. Explain how blockchain lets a transaction be traced. [2]

10 Can I do this?

0 / 2 ticked

- [ ] I can explain what a digital currency is and how it is used.
- [ ] I can describe how blockchain tracks transactions.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER No: only electronically

2.

ANSWER Blockchain

3.

ANSWER The hash of the previous block

Practice: easy, medium, hard

Easy 1.

ANSWER e.g. Bitcoin (a cryptocurrency)

Medium 1.

ANSWER

Each block holds the previous block's hash, so changing one breaks the chain; copies are held on many computers

Hard 1.

ANSWER

Every transaction is stored, time-stamped, in a block that cannot be altered; following the chain shows the history

NOTE 4

Cyber security threats

1 In this note

SYLLABUS 5.3 CYBER SECURITY

- 5.3.1 Describe the processes involved in, and the **aim** of carrying out, a range of cyber security threats: **brute-force attack**, **data interception**, **DDoS**, **hacking**, **malware** (virus, worm, Trojan horse, spyware, adware, ransomware), **pharming**, **phishing**, **social engineering**.

Before this: Digital currency and blockchain. Next: Keeping data safe.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

Packets

Data is sent across a network in packets.

Quick check: can a packet be read on its way?

Yes, if it is intercepted and not encrypted.

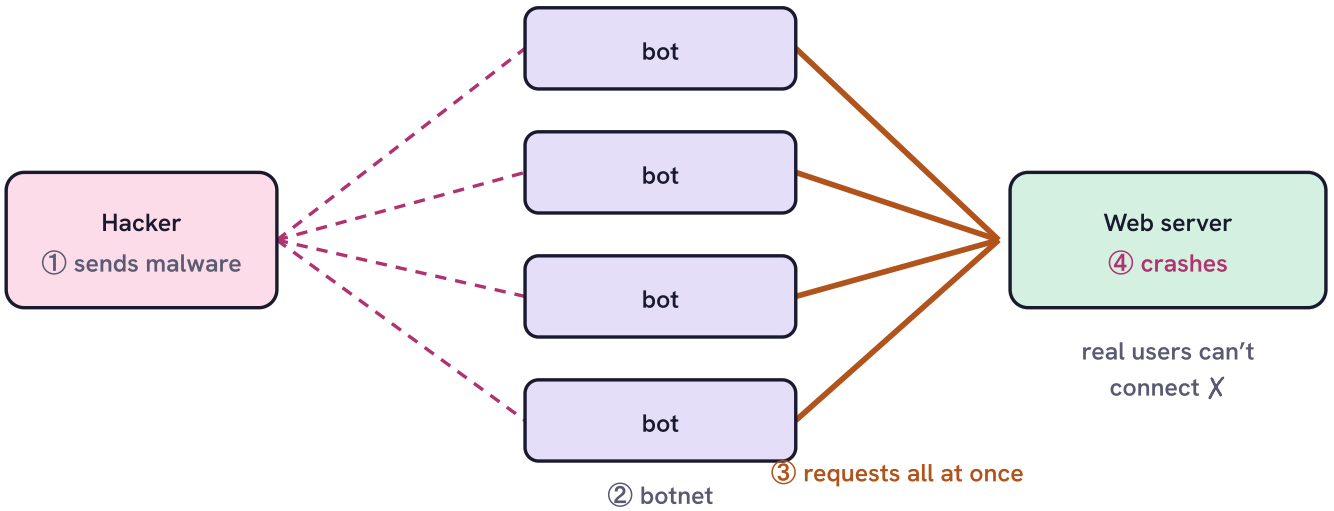
For every threat learn two things: the **process** (how it is done, step by step) and the **aim** (why the attacker does it).

3 Getting into accounts and systems

Threat	Process	Aim
Brute-force attack	**trial and error** to guess a password: combinations are **repeatedly entered** (often automatically by software) **until the correct password is found**	to gain access to an account: steal, view, change or delete data; install malware
Hacking	**gaining unauthorised access** to a computer or system, e.g. by exploiting a weakness	to steal, change or delete data; damage a company's reputation; install malware
Data interception	data is **examined while it is being transmitted**, e.g. with a **packet sniffer**, and copied to a third party, who analyses it	to steal data such as passwords or bank details

4 Denial of service

In a **distributed denial of service (DDoS)** attack, many computers send so many requests to a web server that it cannot cope.



A DDoS attack.

GENERAL METHOD **Process of a DDoS attack**

1. The attacker spreads **malware** that users download onto their computers.
2. Each infected computer becomes a **bot** (zombie); together they form a **botnet**.
3. When the attacker starts the attack, all the bots send **requests to the web server at the same time**.
4. The web server is overloaded and **crashes** / slows, so **real users cannot access the website**.

Aims: to stop a business trading, damage its reputation, revenge, demand a ransom to stop the attack.

5 Malware

Malware (malicious software) is software designed to damage a computer or steal data.

Malware	What it does
Virus	software that **replicates** when the user runs it (it needs an active host program); **deletes, damages or corrupts** data and files; fills storage
Worm	**replicates itself across a network** **without user input**; uses up **bandwidth**; can open back doors and carry other malware
Trojan horse	malware **hidden inside / disguised as genuine software**; when installed, the hidden malware is installed too
Spyware	**records what the user does**, e.g. all key presses (**keylogger**), and **sends it to a third party**, who looks for passwords
Adware	**displays unwanted adverts**; may redirect to fake websites or contain other malware; slows the device
Ransomware	**encrypts the user's data** (locks them out) and demands a **ransom** for the key

> Virus vs worm: a **virus** needs the user to run its host program; a **worm** spreads across a network **on its own**. Phishing is **not** malware.

6 Tricking the user

Threat	Process	Aim
Phishing	a **legitimate-looking email** is sent; the user **clicks a link** in it (or replies) and is taken to a **fake website**, where they **enter personal data**, which is stolen	to obtain personal data: passwords, bank details
Pharming	**malicious code is downloaded** onto the user's computer (or a DNS is changed). When the user **types a genuine web address**, they are **redirected to a fake website**, where they enter personal data	to obtain personal data
Social engineering	**manipulating or deceiving people** into giving away data or making a security mistake, e.g. a phone call pretending to be the bank, or leaving an infected USB stick to be found	to obtain data or access

✗ COMMON MISTAKE

Phishing vs pharming: in **phishing** the user **clicks a link** in an email. In **pharming** the user types the **correct URL** but malware redirects them anyway, so it is harder to spot.

TRY IT YOURSELF

1. Which malware encrypts your files and demands payment?
2. Which malware spreads across a network without the user doing anything?
3. Which threat uses trial and error to guess a password?
4. Is phishing a type of malware?

7 Summary

- Brute force: trial and error until the password is found. Hacking: unauthorised access. Interception: packet sniffer reads data in transit.
- DDoS: malware → bots → botnet → simultaneous requests → server crashes.
- Malware: virus (needs host), worm (spreads itself), Trojan (disguised), spyware (keylogger), adware, ransomware (encrypts, ransom).
- Phishing: email link → fake site. Pharming: malware redirects a typed URL. Social engineering: manipulating people.

IF YOU SEE …

"draw and annotate a diagram to represent a DDoS" [6]	→ malware · bots · botnet · third party starts it · simultaneous requests · server fails · users can't connect
"describe the process of phishing" [4]	→ legitimate-looking email · clicks link · fake website · enters personal data · stolen

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

8 Ways they test it

TYPE 1 **Describe a process**

> *"Describe how a brute-force attack can be used to gain access" [3]; "describe the process of phishing" [4]*

Spot it "describe how / process".

1. Steps in order, from the tables and methods.

TYPE 2 **Diagram**

> *"Draw and annotate a diagram to represent pharming / DDoS / data interception" [4-6]*

Spot it "diagram".

1. Boxes for the computers and servers; an arrow per step, each with a label saying what happens.

TYPE 3 **Aims**

> *"State two aims of carrying out a DDoS attack" [2]*

Spot it "aims".

1. Why, not how.

TYPE 4 **Malware table**

> *"Identify and describe two other examples of malware" [6]*

Spot it "malware".

1. Name + two description points each.

9 What the examiner looks for

"Draw and annotate a diagram to represent the process of pharming" [4]

Marking points (one mark each, up to the marks shown)

- User clicks / opens an attachment or link that triggers a download
- Malicious software is downloaded onto the user's computer
- User enters the (genuine) website address
- User is redirected to a fake website

KEYWORDS **malware downloaded** **enters web address** **redirected** **fake website**

10 Past-paper questions, solved

2210/11/M/J/23 Q8 ↗ Paper 1 · Computer systems **10 marks** ⤢ Full size

8 A manager at a company is concerned about a brute-force attack on its employee user accounts.

(a) Describe how a brute-force attack can be used to gain access to the employee user accounts.

..... [3]

(b) One possible aim for carrying out a brute-force attack is to install malware onto the company network.

(i) State **two** other aims for carrying out a brute-force attack to gain access to the employee user accounts.

[2]

(ii) Identify **three** types of malware that could be installed.

[3]

(c) Give **two** security solutions that could be used to help prevent a brute-force attack being successful.

[2]

Swipe sideways to read the whole question

How to start (a) the process, (b)(i) aims other than installing malware, (b)(ii) three malware names, (c) two solutions (next note).

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) The attacker uses trial and error to guess the password: combinations are repeatedly entered, often automatically by software, until the correct password is found.

(b)(i) To steal data; to delete or change data. (ii) Virus; worm; ransomware.

(c) Two-step verification; limiting the number of login attempts.

PART	ANSWER / WORKING	MARKS	GUIDANCE
8(a)	trial and error · combinations repeatedly entered · until correct · manual or automatic	B3	
8(b)(i)	Any two: steal / view data · delete · change · lock account / encrypt · damage reputation	B2	
8(b)(ii)	Any three: virus · worm · Trojan horse · spyware · adware · ransomware	B3	
8(c)	Any two: two-step verification · biometrics · firewall / proxy · strong password · limit attempts · drop-down boxes · partial password	B2	

Total: 10 marks

0478/13/M/J/23 Q8 ↗ Paper 1 · Computer systems **5 marks** ⤢ Full size

8 Complete the statements about a distributed denial of service (DDoS) attack.

Use the terms from the list.

Some of the terms in the list will **not** be used. You should only use a term once.

anti-virus	bot	botnet	hacker
internet	malware	secondary storage	
spyware	web browser	web server	website

The attacker encourages people to download ..... onto their computer. This will turn each computer into a ..... , creating a network called a ..... .

When the attacker wants the DDoS to take place, repeated requests are simultaneously sent from the computers to a ..... . This causes it to crash, meaning that users can no longer access the ..... that is stored on this hardware.

[5]

Swipe sideways to read the whole question

How to start Follow the DDoS method: malware → bot → botnet → server → website.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

The attacker encourages people to download **malware** onto their computer. This will turn each computer into a **bot**, creating a network called a **botnet**. ... repeated requests are simultaneously sent from the computers to a **web server**. This causes it to crash, meaning that users can no longer access the **website** that is stored on this hardware.

PART	ANSWER / WORKING	MARKS	GUIDANCE
8	malware · bot · botnet · web server · website	B5	

Total: 5 marks

0478/11/O/N/25 Q4 ↗ Paper 1 · Computer systems **6 marks** ⤢ Full size

4 A computer game development company are reviewing their current security solutions.

The company wants employees to be aware of how they can identify phishing.

(a) Describe the process of phishing.

..... [4]

(b) Give **two** ways an employee could identify phishing.

[2]

Swipe sideways to read the whole question

How to start (a) four steps. (b) two checks a user can make.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

(a) A legitimate-looking email is sent to the user. The user clicks a link in the email and is directed to a fake website. The user enters their personal data, which is then stolen and used by a third party.

(b) Check the email address it was sent from; check the URL attached to the link (also: check the spelling and tone).

PART	ANSWER / WORKING	MARKS	GUIDANCE
4(a)	legitimate-looking email · clicks link / replies · fake website · enters personal data · stolen / used by third party	B4	
4(b)	Any two: check sender's email address · check tone / spelling · check the URL of the link	B2	

Total: 6 marks

11 Common mistakes

✗ "Phishing is a virus"	✓ "Phishing is a trick using a fake email; it is not malware"
✗ "A DDoS hacks the server"	✓ "A DDoS floods the server with requests so it crashes"
✗ "Spyware deletes files"	✓ "Spyware records key presses and sends them to a third party"
✗ Mixing up phishing and pharming	✓ phishing = email link; pharming = redirected from a typed URL

12 Practice

Practice: easy, medium, hard

1. Which threat makes a botnet?
2. Which malware is disguised as genuine software?
1. Describe what is meant by social engineering, with an example. [3]
2. State the aim of pharming.
1. Explain why pharming is harder for a user to spot than phishing. [2]

13 Can I do this?

0 / 4 ticked

- [ ] I can describe brute force, hacking and data interception, with aims.
- [ ] I can describe and draw a DDoS attack.
- [ ] I can describe the six types of malware.
- [ ] I can describe phishing, pharming and social engineering.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER Ransomware

2.

ANSWER Worm

3.

ANSWER Brute-force attack

4.

ANSWER No

Practice: easy, medium, hard

Easy 1.

ANSWER DDoS (distributed denial of service)

Easy 2.

ANSWER Trojan horse

Medium 1.

ANSWER

Manipulating / deceiving people to give away data or make an error; e.g. a call pretending to be the bank asking for a PIN

Medium 2.

ANSWER To obtain personal data

Hard 1.

ANSWER

The user types the genuine URL themselves, but is redirected; there is no suspicious email or link to notice

NOTE 5

Keeping data safe

1 In this note

SYLLABUS 5.3 CYBER SECURITY

- 5.3.2 Explain how a range of solutions help keep data safe: **access levels**, **anti-malware**, **authentication** (username and password, biometrics, two-step verification), **automating software updates**, **checking spelling and tone**, **checking the URL**, **firewalls**, **privacy settings**, **proxy-servers**, **SSL**.

Before this: Cyber security threats.

PART 1

Learn the topic

The notes: every idea from the start, with our own examples.

2 What you should already know

The threats

Brute force, hacking, interception, DDoS, malware, phishing, pharming, social engineering.

Quick check: which threat does encryption defend against?

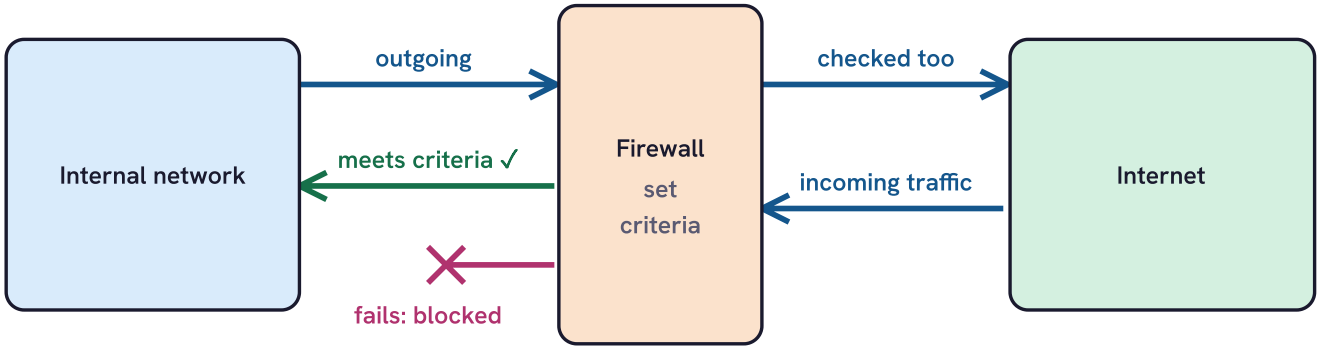
Data interception: intercepted data is meaningless.

3 Authentication and access

Authentication means proving that a user is who they claim to be.

Solution	How it keeps data safe	Helps against
Username and password	only someone who knows the password gets in. A **strong password** (mix of letters, numbers, symbols) is very hard to guess; **limiting login attempts** stops repeated guessing	brute force, hacking
Biometrics	uses a unique physical feature (fingerprint, face, iris, voice); very difficult to fake	brute force, hacking
Two-step verification	after the password, a **code is sent to the user's registered device** (or email) and must be entered: a hacker would need that device too	brute force, hacking, phishing
Access levels	give users **different permissions**: some can only **read** certain data, some can **edit or delete** it; linked to the username	limits the damage any one account can do
Privacy settings	control **who can see** a user's personal information (e.g. on social media)	social engineering, identity theft

4 Software and network defences



Traffic in BOTH directions is compared with the criteria.

How a firewall works.

Solution	How it keeps data safe
Firewall (hardware or software)	sits between a network / computer and the internet; **examines all incoming and outgoing traffic**, **compares it with set criteria** (rules) and **blocks** any that does not meet them; can block certain IP addresses or websites
Proxy-server	sits between users and the internet / a web server: **examines each request**; can **limit the rate of requests** (stopping a DDoS reaching the web server); **hides the server's / user's IP address**; **caches** web pages to answer requests itself
Anti-malware (anti-virus, anti-spyware)	**scans** files and downloads, compares them with a database of known malware, and **quarantines or deletes** malware it finds; anti-spyware stops keyloggers sending passwords
Automating software updates	updates are installed automatically, so **security weaknesses are fixed** as soon as possible and anti-malware always knows the latest malware
SSL (secure socket layer)	**encrypts** data sent between browser and web server; checks the server's **digital certificate**; intercepted data is **meaningless**

5 What the user can check

Solution	How it keeps data safe
Checking the spelling and tone of communications	phishing emails often have spelling mistakes or an urgent, threatening tone ("your account will be closed today")
Checking the URL attached to a link	hover over a link before clicking: a fake site's address is often slightly different (examp1e-bank.com) or not HTTPS

Threat	Best solutions
brute-force attack	strong password · limit login attempts · two-step verification · biometrics
data interception	encryption / SSL (HTTPS)
DDoS	proxy-server · firewall · anti-malware on users' computers
hacking	firewall · strong passwords · two-step verification · access levels
malware	anti-malware · firewall · automatic updates · only download from trusted sources
phishing / pharming	check the URL · check spelling and tone · anti-malware (pharming) · never give personal details
social engineering	staff training · privacy settings · never give data to unverified callers

TRY IT YOURSELF

1. Which solution sends a code to your phone after you enter your password?
2. Which solution makes intercepted data meaningless?
3. Which solution can limit the number of requests reaching a web server?

6 Summary

- Authentication: password (strong, limited attempts), biometrics, two-step verification.
- Access levels: read / edit permissions. Privacy settings: who sees your data.
- Firewall: compares traffic both ways with criteria, blocks what fails.
- Proxy: examines and rate-limits requests, hides IP, caches. Anti-malware: scans, quarantines, deletes.
- Auto-updates fix weaknesses. SSL encrypts. Users: check spelling / tone and the URL.

IF YOU SEE …

"explain how the firewall operates" [5]	→ monitors traffic in and out · set criteria / rules · compares · blocks / allows · can block IP addresses / sites
"identify two solutions and explain how each helps" [6]	→ name (1) + two points of how it stops the attacker

PART 2

How it is examined

Question types, what the examiner gives marks for, and real past-paper questions solved.

7 Ways they test it

TYPE 1 Solution + explanation

> *"Identify two security solutions … explain how each helps prevent hackers" [6]*

Spot it "explain how".

1. 1 mark the name, 2 marks how it stops the attack.

TYPE 2 Firewall diagram

> *"Draw and annotate a diagram to demonstrate how a firewall works" [4]*

Spot it "firewall".

1. Traffic both ways, criteria set, compared, rejected / accepted.

TYPE 3 Proxy vs firewall

> *"Identify two similarities and one difference" [3]; "tasks a proxy performs that a firewall does not" [2]*

Spot it "proxy".

1. Both filter traffic / can block IPs. Proxy only: hides the IP, caches pages.

TYPE 4 Match to a threat

> *"Give two solutions that could prevent a brute-force / DDoS attack" [2]*

Spot it a named threat.

1. Use the threat → solution table.

8 What the examiner looks for

"Draw and annotate a diagram to demonstrate how a firewall works" [4]

Marking points (one mark each, up to the marks shown)

- Traffic passing both ways through the firewall
- An indication that criteria are set for the firewall
- Traffic is compared to the criteria
- Traffic being rejected if it does not meet the criteria
- Traffic being accepted if it meets the criteria

KEYWORDS **both ways** **criteria** **compared** **rejected** **accepted**

9 Past-paper questions, solved

2210/13/O/N/25 Q4 ↗ Paper 1 · Computer systems **6 marks** ⤢ Full size

4 A cyber security company specialises in security solutions that help prevent hackers being successful.

(a) Identify **two** security solutions that can be provided to help prevent hackers being successful.

Explain how each solution helps prevent hackers being successful.

Solution 1 .....

Explanation .....

Solution 2 .....

Explanation .....

[6]

Swipe sideways to read the whole question

How to start Choose solutions you can explain in two steps each.

▼ Show a full-mark answer and the mark scheme · official marking

WHAT TO WRITE

Solution 1: two-step verification. After the password, a code is sent to the user's registered device, so a hacker who has guessed the password would also need that device.

Solution 2: firewall. It examines incoming traffic and blocks any data that does not meet the set criteria, so the hacker's attempts to connect can be stopped.

PART	ANSWER / WORKING	MARKS	GUIDANCE
4(a)	Per solution: name (1) + two matching points (2), e.g. strong password · limit attempts · biometrics · two-step verification · firewall · anti-spyware	B6	

Total: 6 marks

0478/13/M/J/23 Q6 ↗ Paper 1 · Computer systems **9 marks** ⤢ Full size

6 A student is writing a help guide about how to recognise and avoid the cyber-security threat of pharming.

(a) Give **three** appropriate solutions he could include.

[3]

(b) The student also wants to include information in the help guide about the use of social engineering as a cyber-security threat.

Describe what is meant by social engineering.

Include **one** example of social engineering in your answer.

..... [3]

(c) The student includes information about the security solution of access levels.

Describe what is meant by access levels.

..... [3]

Swipe sideways to read the whole question

How to start (a) three different solutions. (b) two marks of description + an example. (c) three points about permissions.

▼ **Show a full-mark answer and the mark scheme** · official marking

WHAT TO WRITE

(a) Check the URL attached to a link; scan downloads with anti-malware; only download software from trusted sources.

(b) Social engineering is manipulating or deceiving people into giving away data or making a security mistake. For example, someone phones pretending to be from the bank and asks for a PIN.

(c) Access levels give users different permissions for the data: some users can only read certain data, while others can also edit or delete it. They are normally linked to a username.

PART	ANSWER / WORKING	MARKS	GUIDANCE
6(a)	Any three: check spelling / tone · check URL · anti-malware scan · trusted sources only · no personal details · firewall	B3	
6(b)	manipulating / deceiving people … to obtain data / make an error · any suitable example	B3	
6(c)	Any three: different permissions · limit reading / viewing · limit editing / deleting · linked to a username	B3	
			Total: 9 marks

10 Common mistakes

✗ "A firewall removes viruses"

✓ "Anti-malware removes viruses; a firewall blocks traffic that fails its criteria"

✗	✓
"Encryption stops data being intercepted"	"Encryption makes intercepted data meaningless"

It can still be intercepted.

✗	✓
"Use a password" for 3 marks	name it + how it helps + why that stops this attacker

11 Practice

Practice: easy, medium, hard

1. Give one example of biometric data.
2. Which software scans for and removes malware?
1. Explain how automating software updates helps keep data safe. [2]
2. Give two tasks a proxy-server can do that a firewall does not.
1. A school wants teachers to edit grades but students only to view them. Name and explain the solution. [3]

12 Can I do this?

0 / 3 ticked

- [ ] I can explain passwords, biometrics, two-step verification, access levels and privacy settings.
- [ ] I can explain firewalls, proxy-servers, anti-malware, automatic updates and SSL.
- [ ] I can match each threat to suitable solutions.

Anything unticked: revise that section first (each line links to it). All ticked: take the quiz.

Answers

Answers to the "Try it yourself" and practice questions on this page. Try every question first.

Try it yourself 1

1.

ANSWER Two-step verification

2.

ANSWER Encryption (SSL)

3.

ANSWER Proxy-server

Practice: easy, medium, hard

Easy 1.

ANSWER e.g. fingerprint

Easy 2.

ANSWER Anti-malware (anti-virus)

Medium 1.

ANSWER

Updates are installed as soon as released, fixing security weaknesses before attackers can exploit them

Medium 2.

ANSWER Hide the IP address; cache web pages

Hard 1.

ANSWER

Access levels: teachers' accounts get edit permission, students' accounts read-only, linked to each username