

Exercise walk-through

5.3

Cyber security

IGCSE Computer Science

Cyber threats

brute force

try many passwords fast until one works

data interception

“listen in” to steal data in transit

DDoS

flood a server until it cannot respond

malware

virus, worm, Trojan,
spyware, ransomware

phishing / social engineering – trick a person into giving up secrets

Cyber security locks data and systems against malware, phishing and unauthorised access – the padlock is the whole job in one picture.

The cyber-security threats, by what each does

DDoS

flooding a server with so many requests that it **cannot respond**, so the website goes down

hacking

gaining access to a system **without permission**

pharming

secret code sends you to a **fake website even when you type the correct address**

phishing

fake emails or messages that **trick you** into giving away private details

brute-force attack

trying every password until one works

data interception

reading data as it travels across a network

Phishing needs **you** to click; pharming does not. That difference is why one is beaten by care and the other only by technical defences.

Three attacks, and the words behind them

Brute force attack

A **brute force attack** tries every combination until a password works – which is why length beats complexity.

Distributed denial of service

A **distributed denial of service** (DDoS) attack floods a server from many machines at once, so real users cannot get through.

DNS

The **domain name service** turns a name into an IP address; poisoning it sends visitors to the attacker's server instead.

Hash value

A **hash value** is a fixed-length fingerprint of data. Passwords are stored hashed, so a stolen database does not hand over the passwords.

For each threat name the target, the method and one defence. That triple answers almost every question in this topic.

Malware – know the differences

virus	attaches to a file; spreads when opened
worm	spreads over a network on its own
Trojan	pretends to be useful software
spyware	secretly records what you do
ransomware	locks files, demands payment

The key distinction: a **worm** needs no file and no user action – it copies itself across the network. A **virus** needs a file to be opened.

The malware types

virus

attaches to a file and needs a person to run it

worm

copies itself across a network with **no** human action

trojan horse

disguised as something useful, so you install it yourself

spyware

records what you do – often a **keylogger**
you type

capturing what

adware

floods you with unwanted adverts

ransomware

encrypts your files and demands payment for the key

These attacks **steal personal data, delete or change files, stop a service working, cost money, and make users lose trust in a company.**

Exercises 2.1-2.3

2.1 State what a brute force attack is.

[1]

2.2 State what ransomware does.

[1]

2.3 Give the name of the data before and after encryption.

[2]

Exercises 2.1-2.3

2.1 State what a brute force attack is. [1]

2.1

- the attacker tries password after password
- a **brute-force attack** tries many passwords very quickly until one works

2.2 State what ransomware does. [1]

2.2

- ransomware **locks your files and demands payment** to unlock them

2.3 Give the name of the data before and after encryption. [2]

2.3

- before encryption: **plaintext**
- after encryption: **ciphertext**

Exercises 2.4-2.5

2.4 Identify two tasks performed by a proxy server.

[2]

2.5 Explain why encryption does not stop data being intercepted.

[2]

Exercises 2.4·2.5

2.4 Identify two tasks performed by a proxy server. [2]

2.4

- any **two** of: filters traffic / caches web pages / hides the user's IP / acts as a firewall
-

2.5 Explain why encryption does not stop data being intercepted. [2]

2.5

- encryption only **scrambles** the data
- an interceptor can still take a copy, but without the key the ciphertext is **meaningless**

Exercise 3.1

3.1 A firewall protects a network by:

[1]

☐

A scanning for viruses

B checking data in/out and blocking what is not allowed

C encrypting files

D hiding the IP address

Exercise 3.1

3.1 A firewall protects a network by:

[1]

☐

A scanning for viruses

B checking data in/out and blocking what is not allowed

C encrypting files

D hiding the IP address

3.1 B

- a firewall **checks data in/out and blocks what is not allowed**
- A is anti-malware; C is encryption; D is a proxy

Exercise 3.2 (a)

3.2 A company wants to protect its data.

(a) Describe what a phishing attack is.

[2]

Exercise 3.2 (a)

3.2 A company wants to protect its data.

(a) Describe what a phishing attack is.

[2]

(a)

- **fake emails or messages**
- they trick you into **giving away private details**

Exercise 3.2 (b)

3.2 A company wants to protect its data.

(b) State two methods (other than a firewall) to keep data safe.

[2]

Exercise 3.2 (b)

3.2 A company wants to protect its data.

(b) State two methods (other than a firewall) to keep data safe. [2]

(b)

- any **two** of: authentication / anti-malware / access levels / automatic updates / proxy server

Exercise 3.3

3.3 State the difference between a virus and a worm.

[2]

Exercise 3.3

3.3 State the difference between a virus and a worm.

[2]

3.3

- a **virus** attaches to a file and copies itself when the file is opened
- a **worm** copies itself across a network on its own

Exercise 3.4 (a)

3.4 An online bank protects its customers' data.

(a) Explain what happens to data when it is encrypted, using the terms plaintext and ciphertext. [2]

Exercise 3.4 (a)

3.4 An online bank protects its customers' data.

(a) Explain what happens to data when it is encrypted, using the terms plaintext and ciphertext. [2]

(a)

- readable **plaintext** is scrambled with a key into **ciphertext**
- it cannot be understood without the matching key to decrypt it

Exercise 3.4 (b)

3.4 An online bank protects its customers' data.

(b) Identify the protocol that encrypts the connection between a customer's browser and the bank's server, and give one way the customer can tell it is being used. [2]

Exercise 3.4 (b)

3.4 An online bank protects its customers' data.

(b) Identify the protocol that encrypts the connection between a customer's browser and the bank's server, and give one way the customer can tell it is being used. [2]

(b)

- **SSL** or **TLS**
- the address begins with **https**, or a **padlock** is shown

Exercise 3.4 (c)

3.4 An online bank protects its customers' data.

(c) Describe two tasks a firewall performs for the bank's network.

[2]

Exercise 3.4 (c)

3.4 An online bank protects its customers' data.

(c) Describe two tasks a firewall performs for the bank's network. [2]

(c)

- any **two** of: examines traffic in and out / compares with criteria and blocks failures / keeps a log / blocks named sites or IP addresses

Exercise 3.4 (d)

3.4 An online bank protects its customers' data.

(d) Bank staff have different access rights. Explain how access rights protect customer data even from someone who has logged in successfully. [2]

Exercise 3.4 (d)

3.4 An online bank protects its customers' data.

(d) Bank staff have different access rights. Explain how access rights protect customer data even from someone who has logged in successfully. [2]

(d)

- each user is given only the permissions **their job needs**
- a clerk who logs in **cannot open customer files** reserved for managers

Exercise 3.4 (e)

3.4 An online bank protects its customers' data.

(e) The bank adds two-step verification. Describe how it works and explain why it is safer than a password alone. [3]

Exercise 3.4 (e)

3.4 An online bank protects its customers' data.

(e) The bank adds two-step verification. Describe how it works and explain why it is safer than a password alone. [3]

(e)

- after the password is accepted, a **one-time code** is sent to a device the user holds
- the user must enter that code to complete the log-in
- a thief with only the password **cannot get in without the device**

Exercise 3.4 (f)

3.4 An online bank protects its customers' data.

(f) Explain one advantage of asymmetric encryption over symmetric encryption when a customer first connects. [2]

Exercise 3.4 (f)

3.4 An online bank protects its customers' data.

(f) Explain one advantage of asymmetric encryption over symmetric encryption when a customer first connects. [2]

(f)

- the bank publishes a **public key** that anyone may use to encrypt
- **no secret key** has to be sent over the internet, unlike symmetric encryption