Keeping your personal data secure

Version: 1.0

Effini

Data Education in Schools

Skills Development Scotland

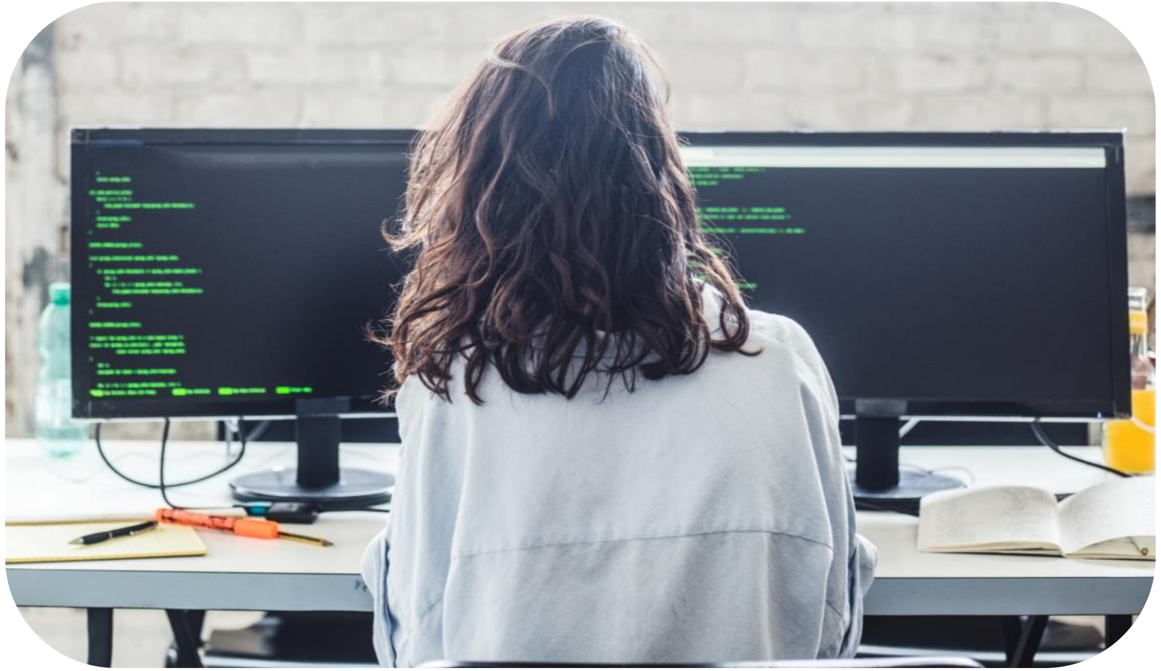
Learning intentions

We will be looking at how you can keep your personal data secure, specifically,

- How to choose and test a **good password**
- How to use a **password manager** and **multi-factor authentication** including biometrics
- How to protect personal devices with **anti-virus software**, **firewalls** and **VPNs**
- How to protect information you share online

Background

If data is private, it is critically important to both individuals and businesses to keep it secure. This will stop it falling into the wrong hands.



Keeping data safe is everybody's responsibility. Human beings are often unknowingly the weakest link in keeping data secure.

In this lesson, we will look at **how you can keep your data secure.**

Definition

Personal data

information that relates to an identified or identifiable individual

Show me…

As well as your name and address, there is lots of personal data that can identify you and needs protecting.

Your turn…

Can you think of **5 types of personal data** that a school, college or employer holds that could be used to identify you? e.g. Date of birth

1.

2.

3.

4.

5.

Your turn…

Here are some examples of personal data a school, college or employer could hold,

1. Videos/photos of you and your work
2. Emails you have been sent
3. Attendance record
4. Emergency contact details
5. Your grades

Why securing personal data is important?

Prevents **your device from being hacked** and your access being blocked

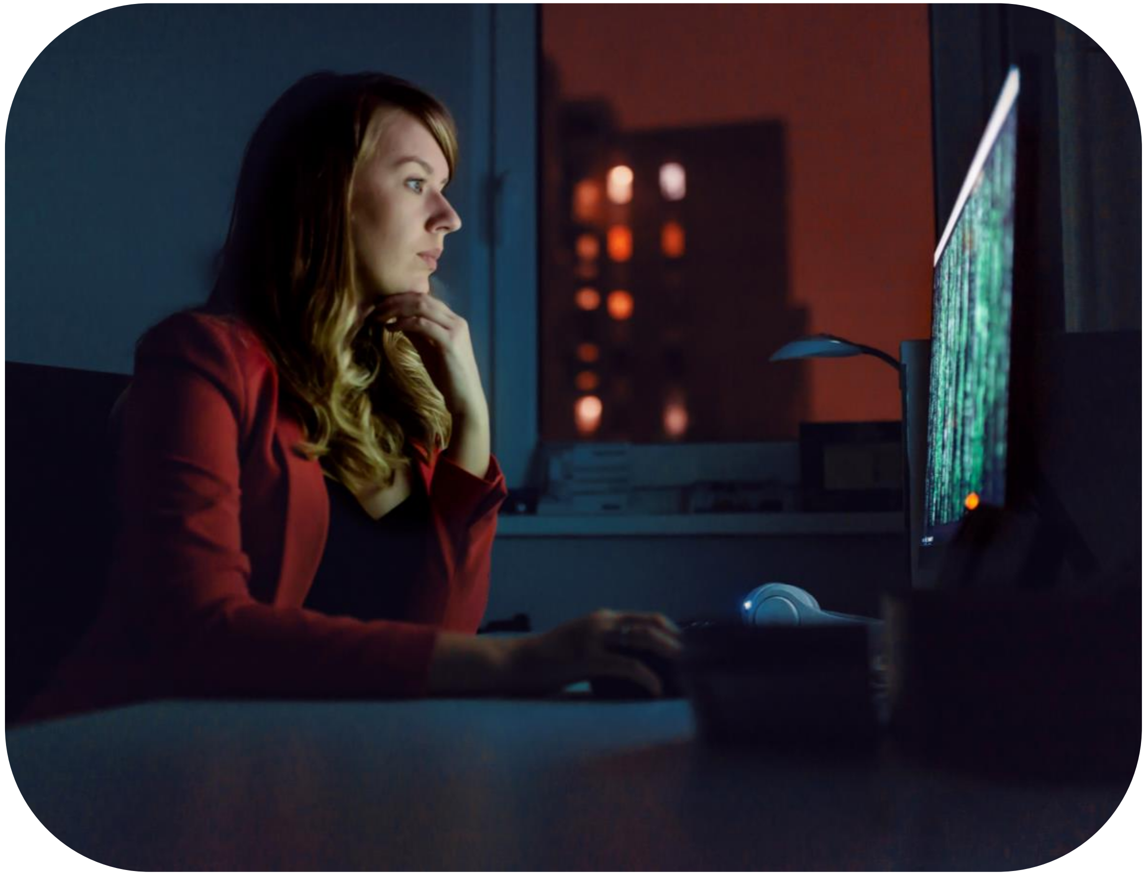
Stops your data being used for **un-ethical reasons**, e.g. to try and influence your vote

Reduces the risk of your **username and password being stolen**

How secure is your personal data?

We are now going to think about different ways of keeping your personal data secure.

As we go through the lesson you can give yourself a score for each section on how well you keep your personal data secure.



Definition

Strong password

combination of letters, numbers and special characters that are difficult to guess by a person or program

Show me…

The table below shows example passwords and how long it would take someone to crack it.

Password	Strength	Time to crack
123456	Very weak	0 secs
Monday2	Very weak	5 secs
awesomedog1	Weak	117 secs
hello_my_fr1end	Medium	40 hours
JanRedRa1nbow$	Strong	13 days
BlueDoorFavWatch	Very strong	14 years
9X#u$4Xg9	Very strong	24,000 years

The strength and time to crack has been calculated on passwordmonster.com

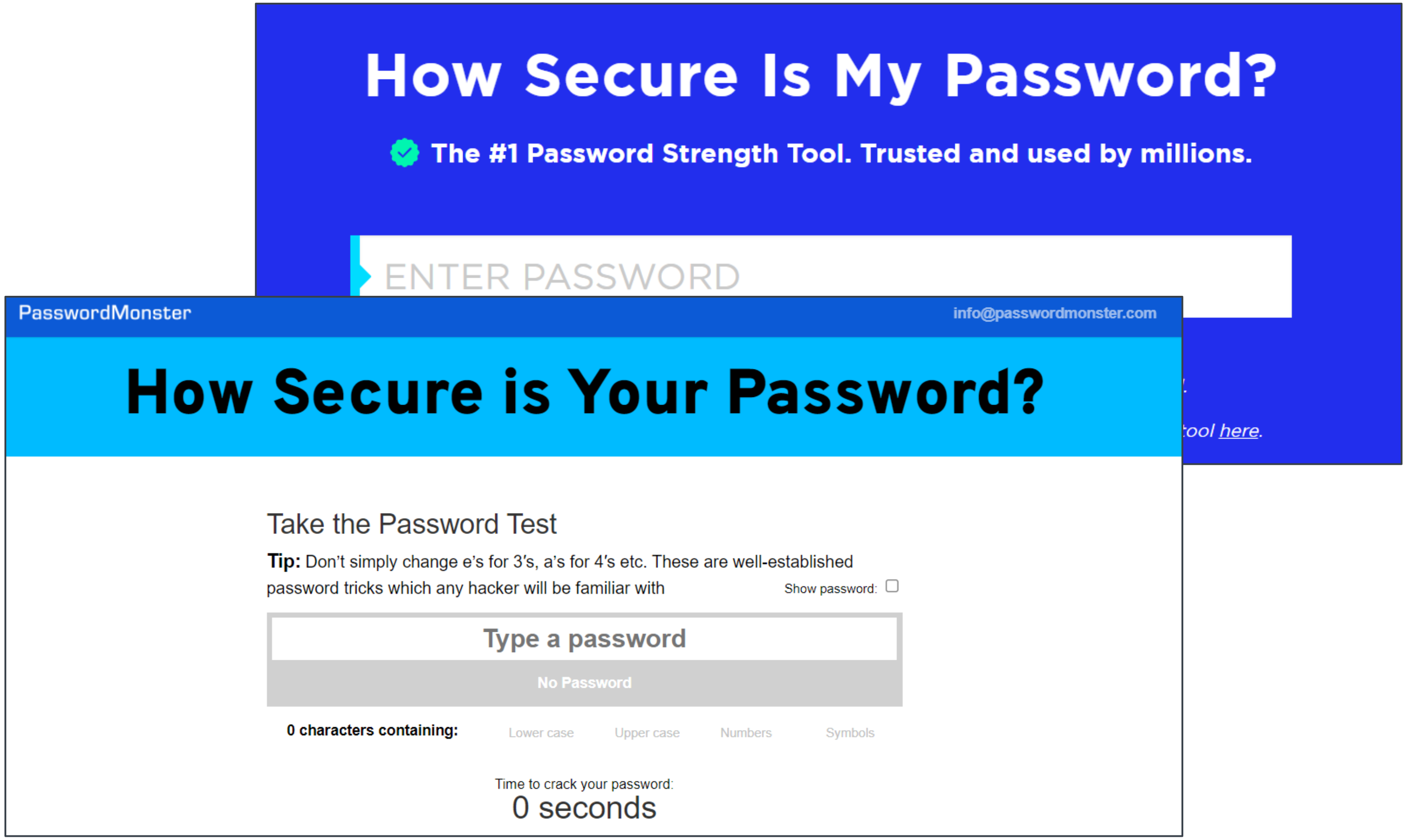
Testing your passwords

There are websites you can use to test the strength of your password such as,

passwordmonster.com

security.org/how-secure-is-my-password/

uic.edu/apps/strong-password/



How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

ENTER PASSWORD

ool *here*.

PasswordMonster info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: □

Type a password

No Password

0 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
0 seconds

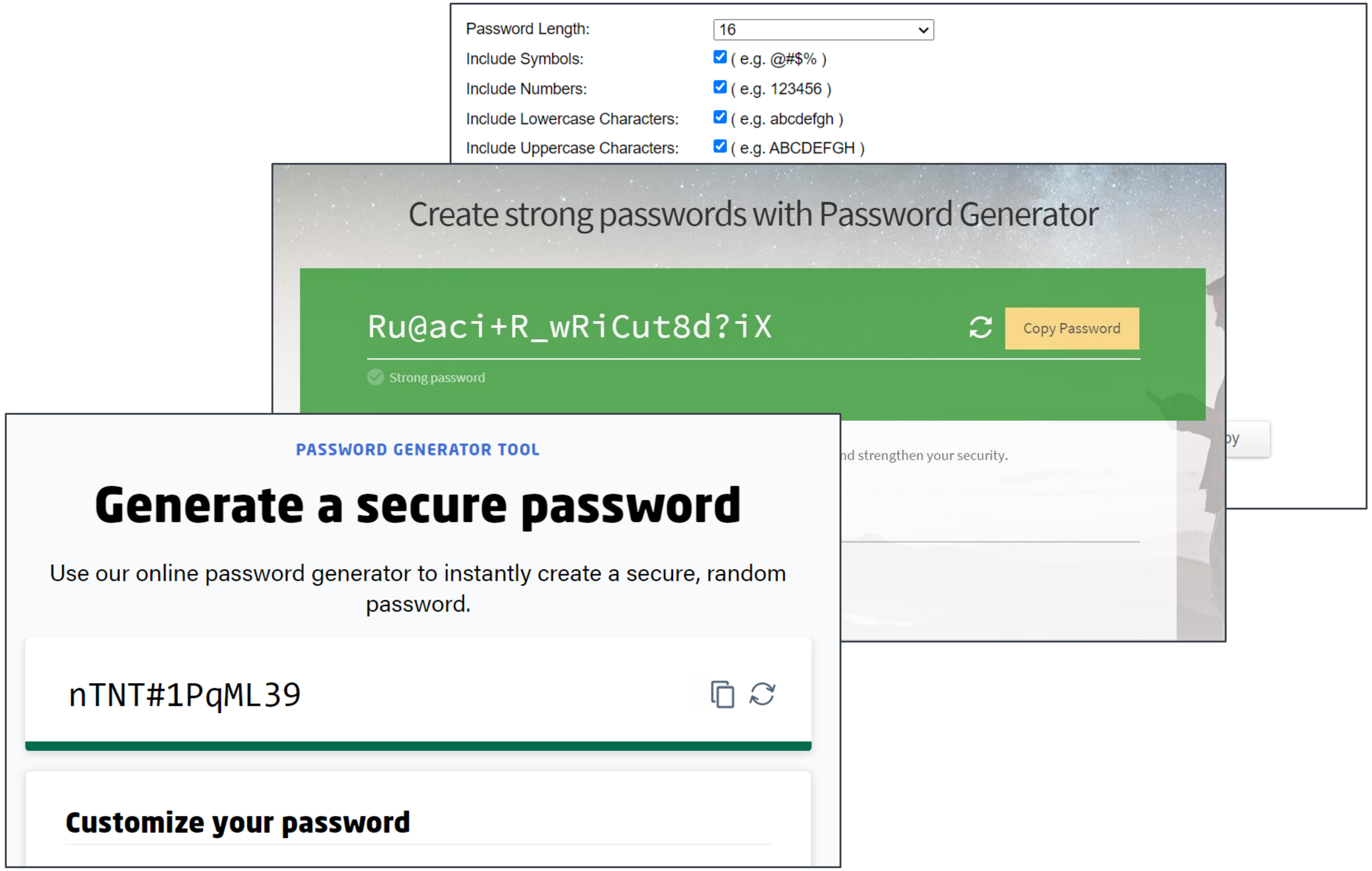
Generating strong passwords

If you need a strong password you can use a website to generate one,

passwordsgenerator.net

lastpass.com/features/password-generator

my.norton.com/extspa/passwordmanager



Password Length:	16
Include Symbols:	☑ (e.g. @#$%)
Include Numbers:	☑ (e.g. 123456)
Include Lowercase Characters:	☑ (e.g. abcdefgh)
Include Uppercase Characters:	☑ (e.g. ABCDEFGH)

Create strong passwords with Password Generator

Ru@aci+R_wRiCut8d?iX

nd strengthen your security.

PASSWORD GENERATOR TOOL

Generate a secure password

Use our online password generator to instantly create a secure, random password.

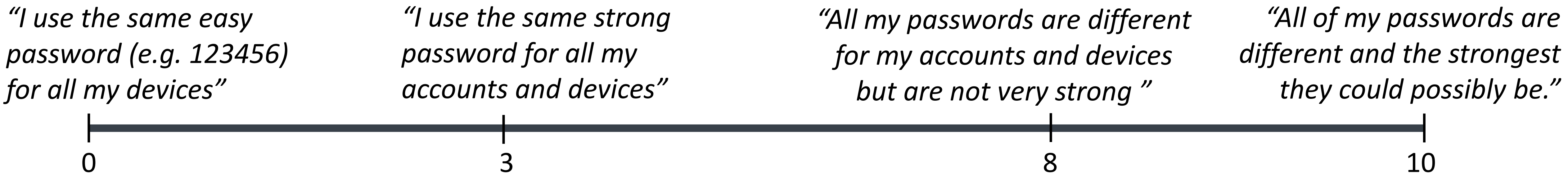
nTNT#1PqML39

Customize your password

Your turn…

Think about the passwords you use on your devises such as your phone or computer.

On a scale of 0 – 10, how **strong do think the passwords** you use are?



"I use the same easy password (e.g. 123456) for all my devices"

"I use the same strong password for all my accounts and devices"

"All my passwords are different for my accounts and devices but are not very strong "

"All of my passwords are different and the strongest they could possibly be."

Your turn…

Keep a note of the score you have given yourself, you will add this to the other scores throughout the lesson to give you a total ‘keeping personal data secure’ score.

Strong password	7
Part 2	?
Part 3	?
Part 4	?
Part 5	?
Part 6	?
Total score	**7/60**

Using a password manager

When you have different, strong passwords for all your accounts, it can be difficult to remember them all.

It is best practice to use a **tool that will remember them for you**.

The tool is secured with a single password, then this is the only password the user needs to remember.

Definition

Password manager

Software that securely stores passwords that a user has for online accounts

Show me…

Using a password manager removes the need to ever remember a password again.

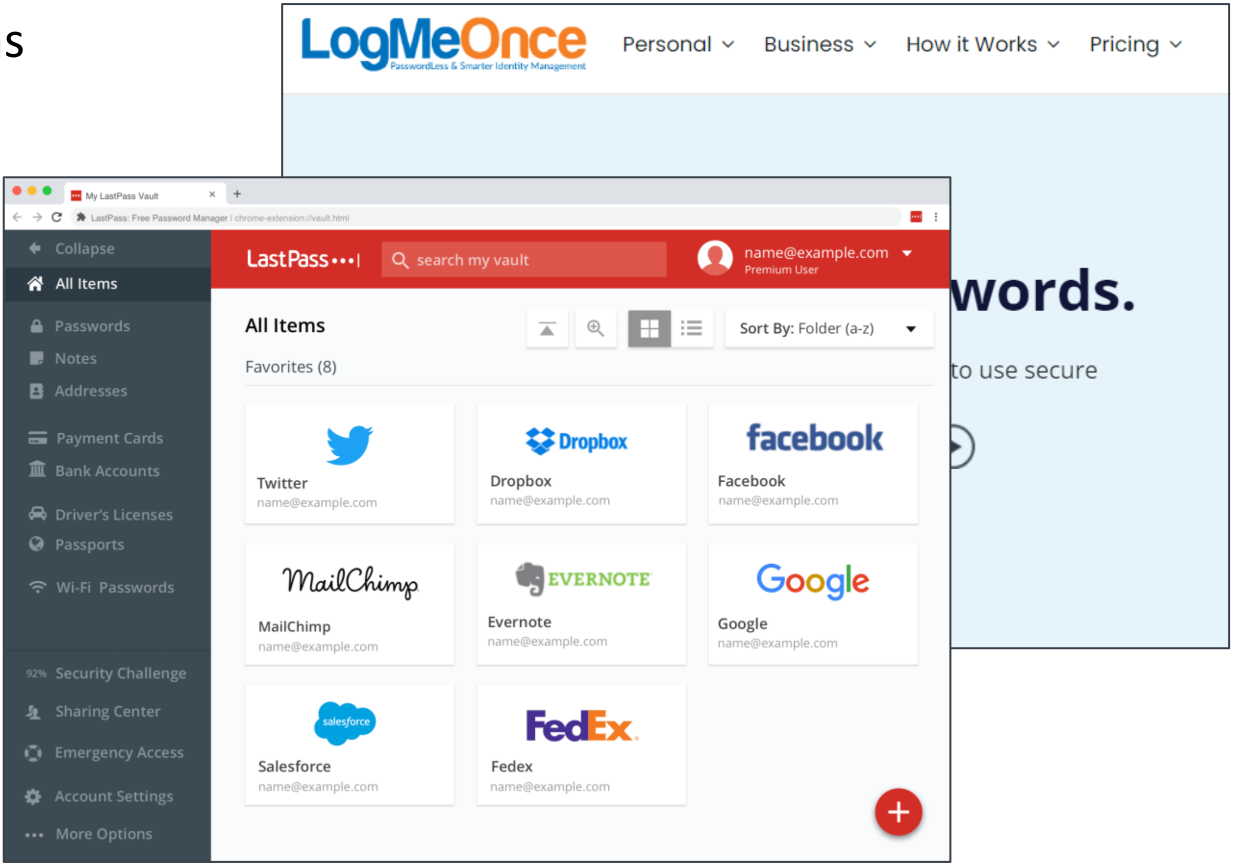
Many password managers are available for free, such as

passwords.google.com

lastpass.com/password-manager

dashlane.com

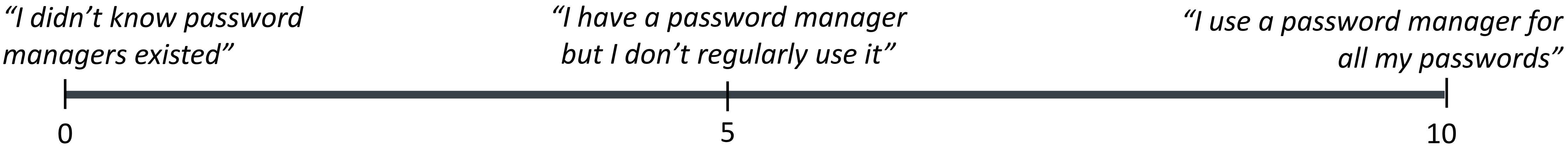
logmeonce.com



Your turn…

Thinking about all the online accounts you have.

On a scale of 0 – 10, how **often do you use a password manager**?



“I didn’t know password managers existed”

“I have a password manager but I don’t regularly use it”

“I use a password manager for all my passwords”

0

5

10

Your turn…

Keep a note of the score you have given yourself, you will add this to the other scores throughout the lesson to give you a total ‘keeping personal data secure’ score at the end.

Strong password	7
Password manager	5
Part 3	?
Part 4	?
Part 5	?
Part 6	?
Total score	**13/60**

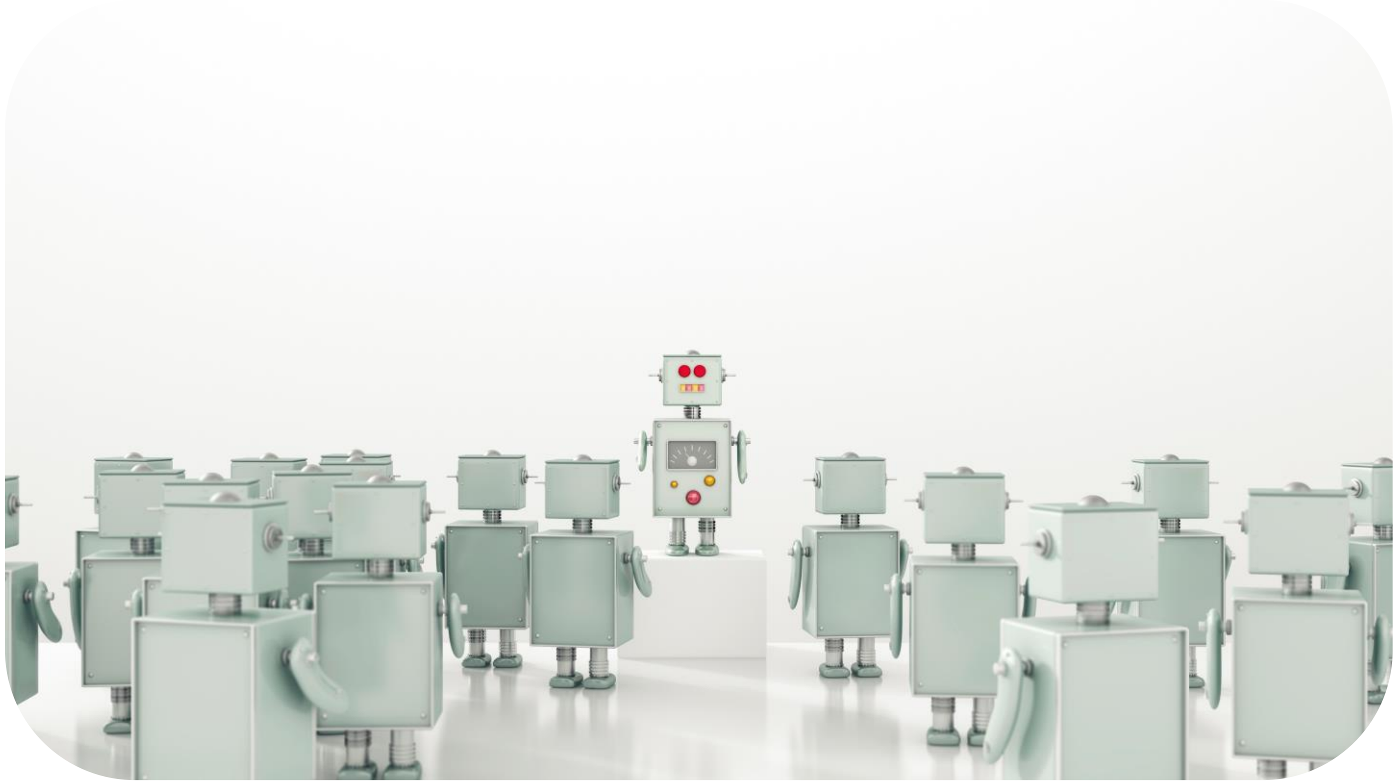
Next steps

Complete **questions 1 to 7**
in **section 1** of the
‘Keeping personal data secure’ workbook.

Extra protection on top of strong password

Even with strong passwords, it is best practice to have **multiple ways of confirming you** are who you say you are.

This means if your password is stolen or cracked, it will be useless to the criminal without them having another way of them trying to show they are you.



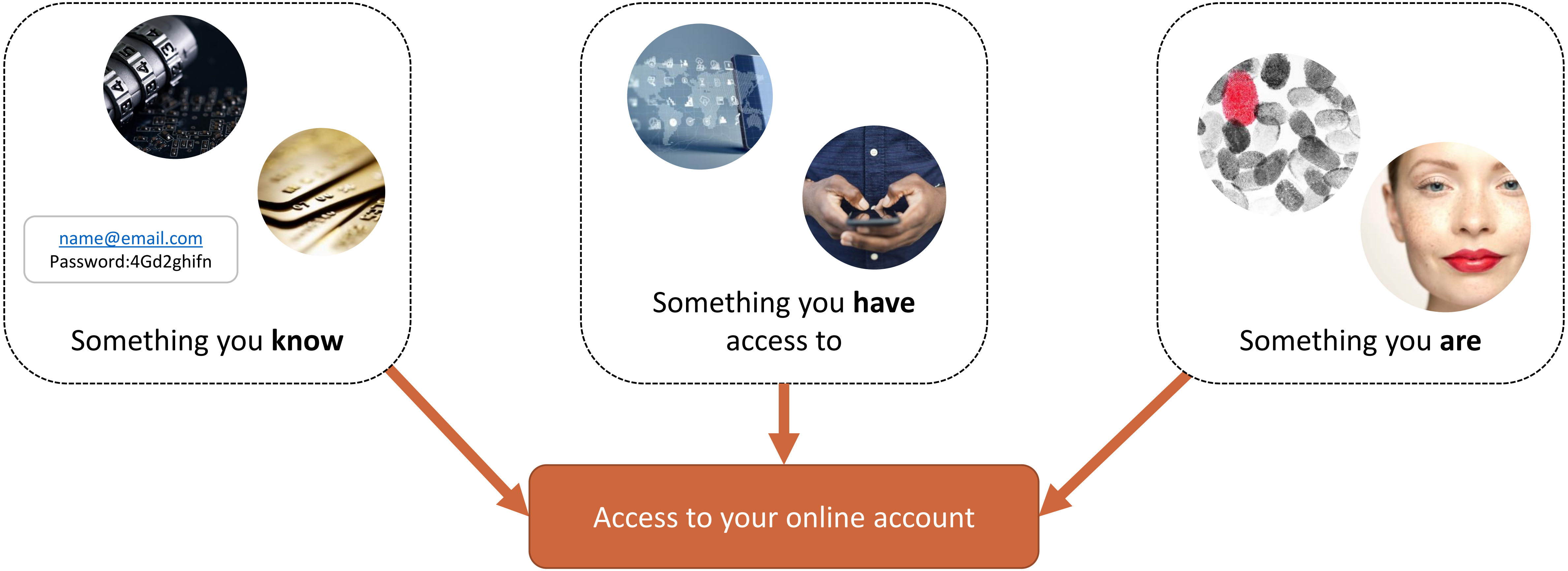
Definition

Multi-factor authentication (MFA)

Two or more pieces of information are required to gain access to an account

Accessing your online accounts

MFA uses a combination of information from different ways of proving your identity. It is unlikely a criminal would have access to your information from all 3 of these types of data.



name@email.com
Password:4Gd2ghifn

Something you **know**

Something you **have** access to

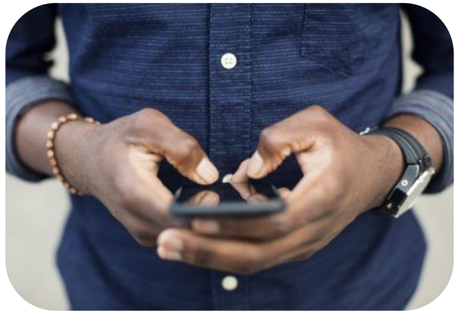
Something you **are**

Access to your online account

Show me…

Below are examples of the types of information you can use to prove your identity to gain access to online accounts.

Password



Enter a code on your phone

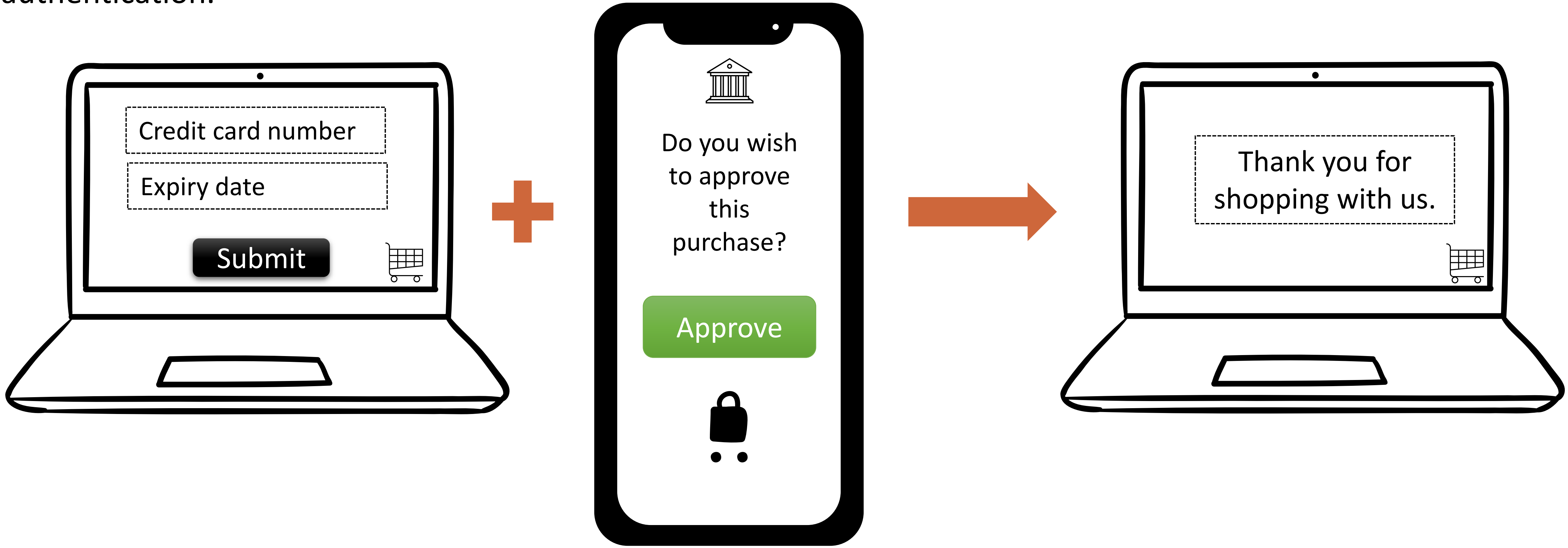
Finger print

Show your location

Authenticator apps

Example

Some times if you are using a credit card online, you may be asked to approve the purchase within your **credit card banking app** as well as entering all the **information from the credit card**. This is multi-factor authentication.


Credit card number
Expiry date
Submit
Do you wish to approve this purchase?
Approve
Thank you for shopping with us.

Definition

Biometrics

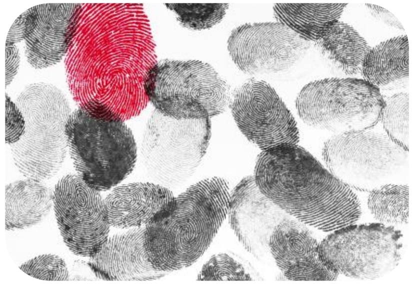
Using a person’s physical or behavioural characteristics to authenticate access

Show me…

Biometrics can use physical or behavioural characteristics to identify a person.

Facial recognition

Iris recognition



Fingerprint scanners

Voice recognition

Hand geometry

Gait

Use of biometrics

Although is convenient for users to access information using biometrics, they are **not yet foolproof.**

Pictures have been successfully used instead of facial recognition, fingerprints can be copied with bluetack and matching can be inaccurate.

Also, if a person's physical characteristics are being stored they can also be stolen/hacked.

However, unlike passwords the user cannot just replace their physical features.

Your turn…

Think about how you access your online accounts.

On a scale of 0 – 10, how often **do you use multi-factor authentication** when logging on to your accounts?

"I didn't know that multi-factor authentication existed"

*"I use MFA on **some** of my accounts."*

*"I use MFA **on all** my online accounts."*

0

5

10

Your turn…

Keep a note of the score you have given yourself, you will add this to the other scores throughout the lesson to give you a total ‘keeping personal data secure’ score at the end.

Strong password	7
Password manager	5
Multi-factor authentication	4
Part 4	?
Part 5	?
Part 6	?
Total score	**16/60**

Next steps

Complete **questions 1 to 7**

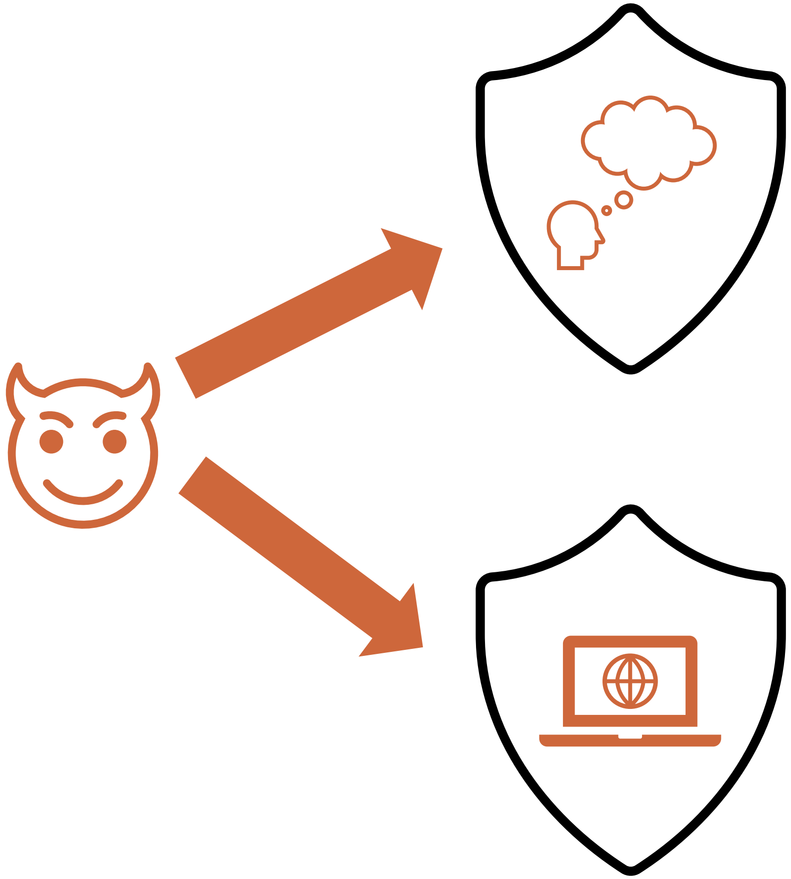
in **section 2** of the

‘Keeping personal data secure’ workbook.

Keeping your devices secure

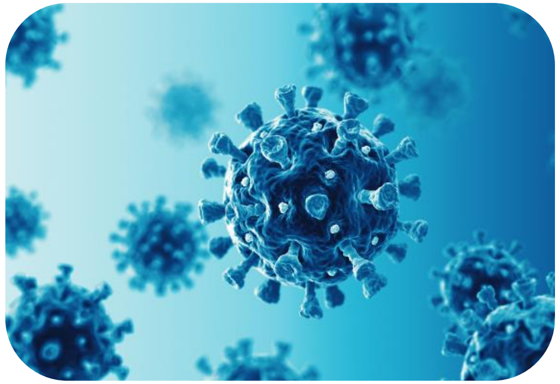
As well as protecting your username and passwords when logging on online accounts, it is important to secure any computer and phones you use from potential risks.

If you access your accounts on a computer that is not secure then you are still at risk.



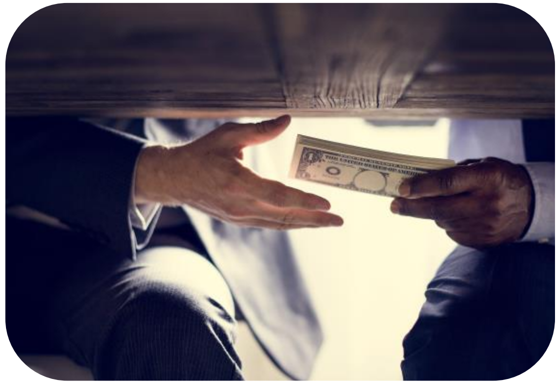
What can cause damage to your device?

Malware (malicious software) is unauthorised software that can end up on a computer and then cause damage. You can use software to protect your devices from these risks.



Virus

Worms



Ransomware

Spyware or
Trojan horses

Definition

Anti-virus software

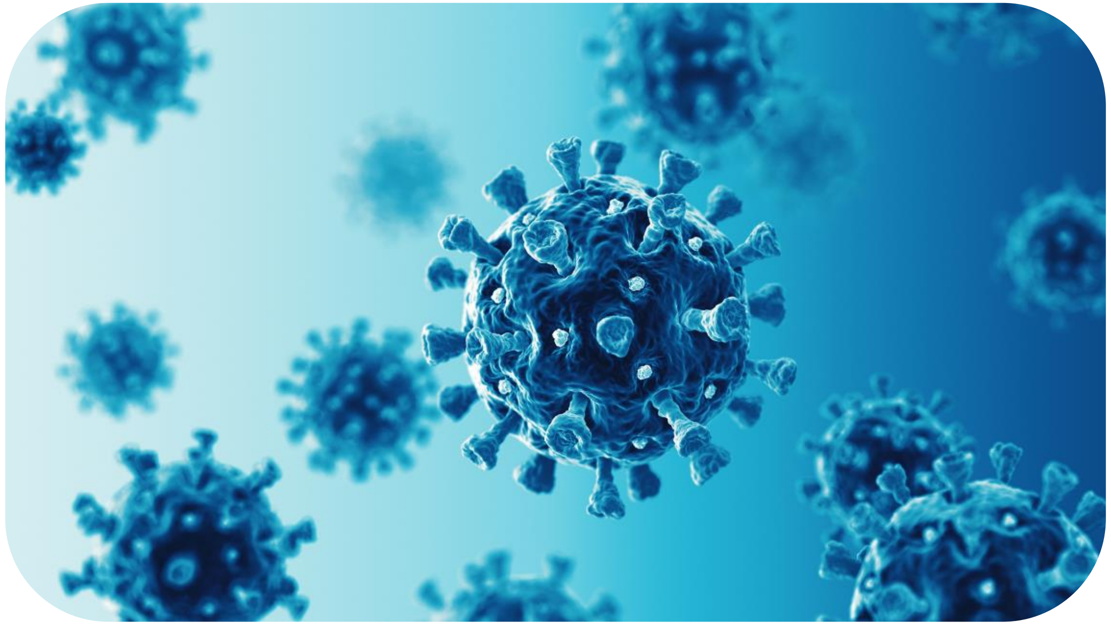
Software designed to detect and destroy computer viruses

Preventing software viruses

Antivirus software prevents files that contain known malware from being downloaded to a computer.

Most good antivirus software also have the ability to remove malware if it is detected.

It is important both to **install a virus-checker** on all computers and devices and **run scans regularly.**



Show me…

Some examples of popular antivirus software providers are given below.

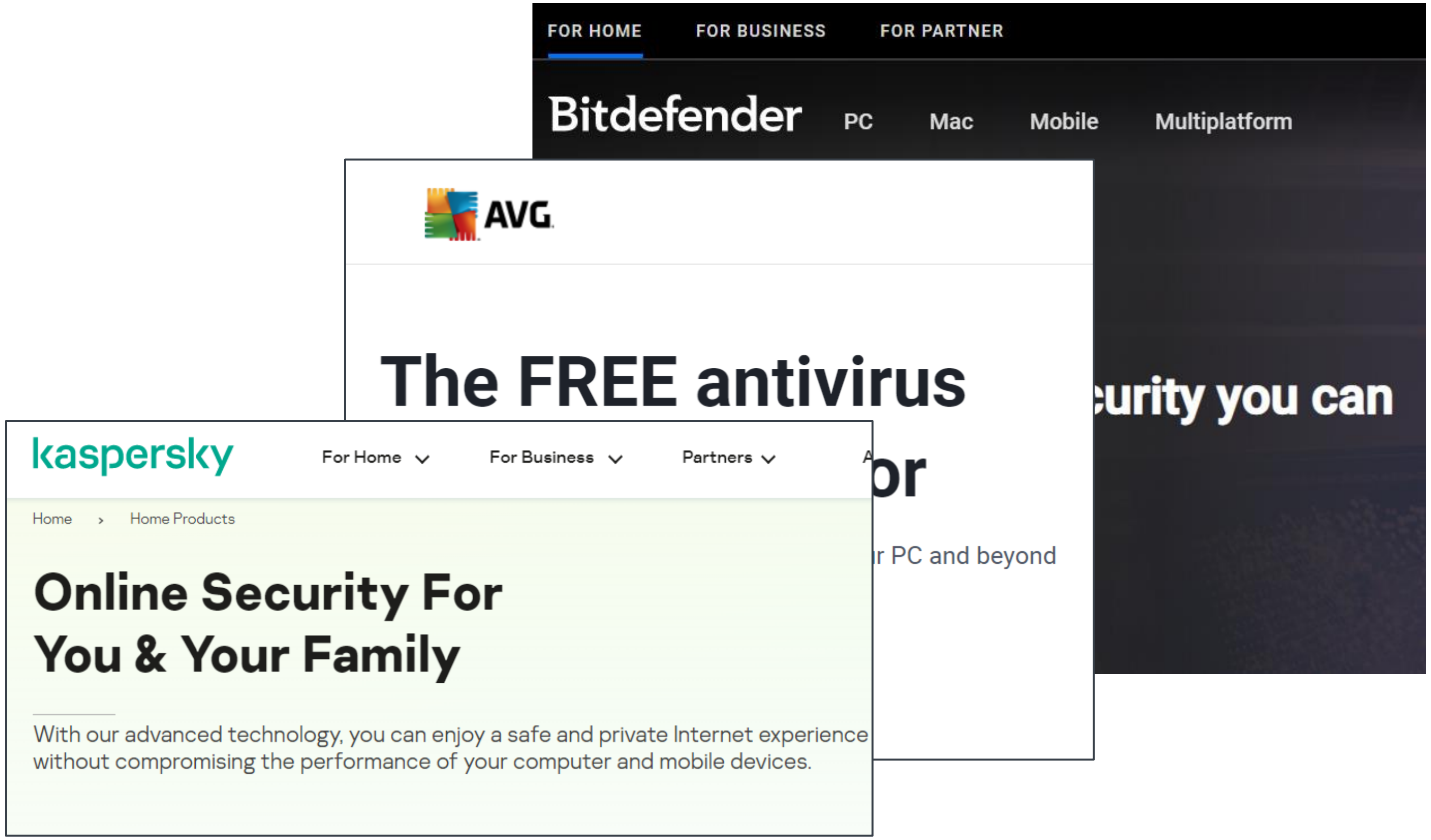
[Avast]

[Bitdefender]

[AVG]

[Kaspersky]

[TotalAV]



curity you can

The FREE antivirus

or

r PC and beyond

Online Security For You & Your Family

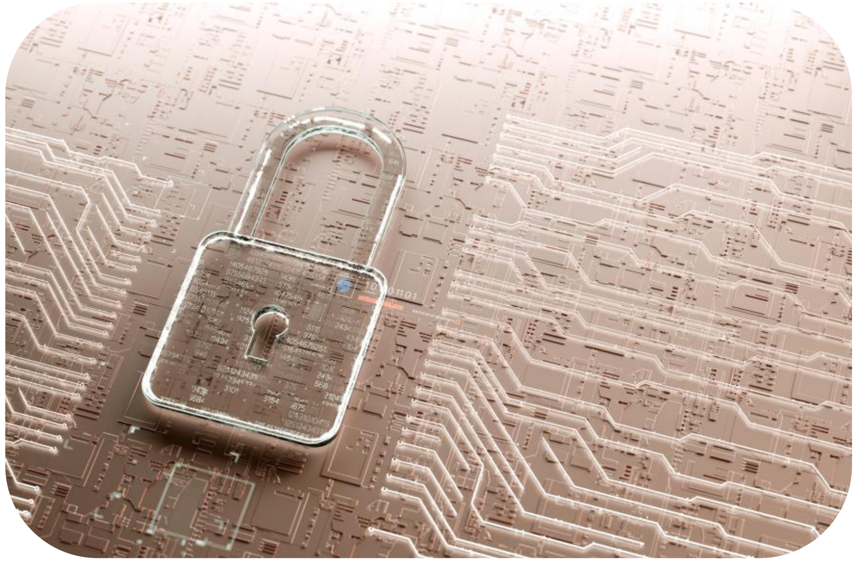
With our advanced technology, you can enjoy a safe and private Internet experience without compromising the performance of your computer and mobile devices.

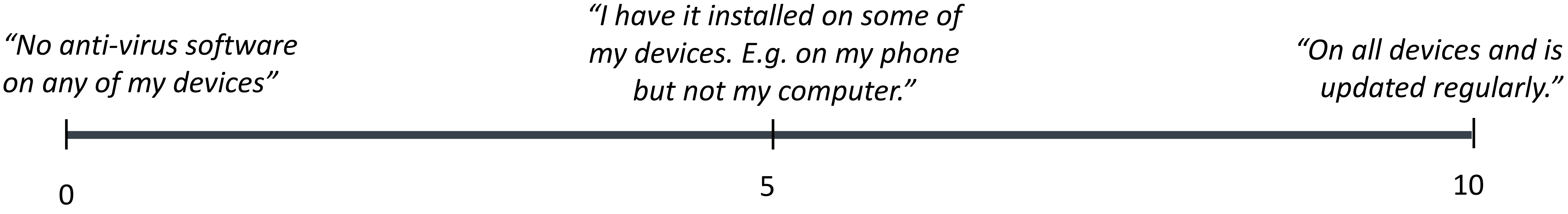
Some anti-virus software is free. However, with anything free, care should be taken to ensure there is not a hidden cost in the sharing of user data for example, or in the loss of critical features.

Your turn…

Thinking about all the devices you use when you connect to the internet.

On a scale of 0 – 10, do you have **update anti-virus software** that runs regular scans on all your devices?





“No anti-virus software on any of my devices”

“I have it installed on some of my devices. E.g. on my phone but not my computer.”

“On all devices and is updated regularly.”

Your turn…

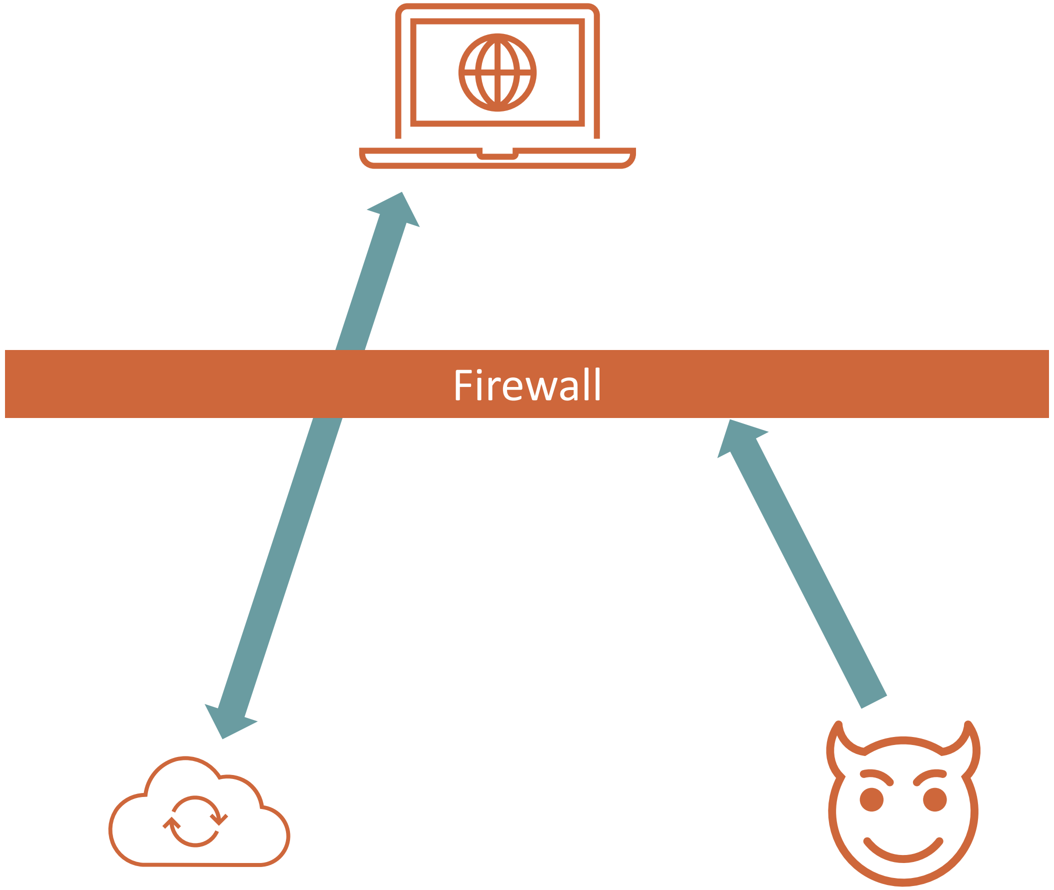
Keep a note of the score you have given yourself, you will add this to the other scores throughout the lesson to give you a total ‘keeping personal data secure’ score at the end.

Strong password	7
Password manager	5
Multi-factor authentication	8
Anti-virus	3
Part 5	?
Part 6	?
Total score	**23/60**

Extra layer of protection to your device

Even if you have up to date anti-virus software on all your devices, you can add an extra layer of protection by using software that blocks unwanted traffic coming on to your device.

This is called a **firewall**.



Definition

Firewall

Security software that restricts unwanted incoming and outgoing internet traffic

Enable firewalls

Firewalls are the gatekeepers to a computer from the internet. It is designed to block unwanted traffic from flowing through it and can be hardware or software.

Most **modern operating systems come with a software firewall automatically enabled**, but it is good practice to check this.

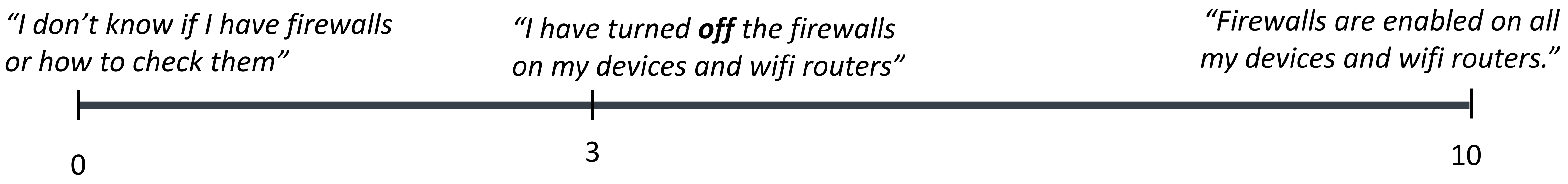
Most **wifi routers also have an inbuilt firewall.** It is worth checking this is also enabled.

Why do you think it's called a firewall?

Your turn…

Thinking about your devices and any wifi routers you use.

On a scale of 0 – 10, do you have **all firewalls enabled**?



"I don't know if I have firewalls or how to check them"

*"I have turned **off** the firewalls on my devices and wifi routers"*

"Firewalls are enabled on all my devices and wifi routers."

0

3

10

Your turn…

Keep a note of the score you have given yourself, you will add this to the other scores throughout the lesson to give you a total 'keeping personal data secure' score at the end.

Strong password	7
Password manager	5
Multi-factor authentication	8
Anti-virus	3
Firewall	10
Part 6	?
Total score	**33/60**

Next steps

Complete **questions 1 to 4**

in **section 3** of the

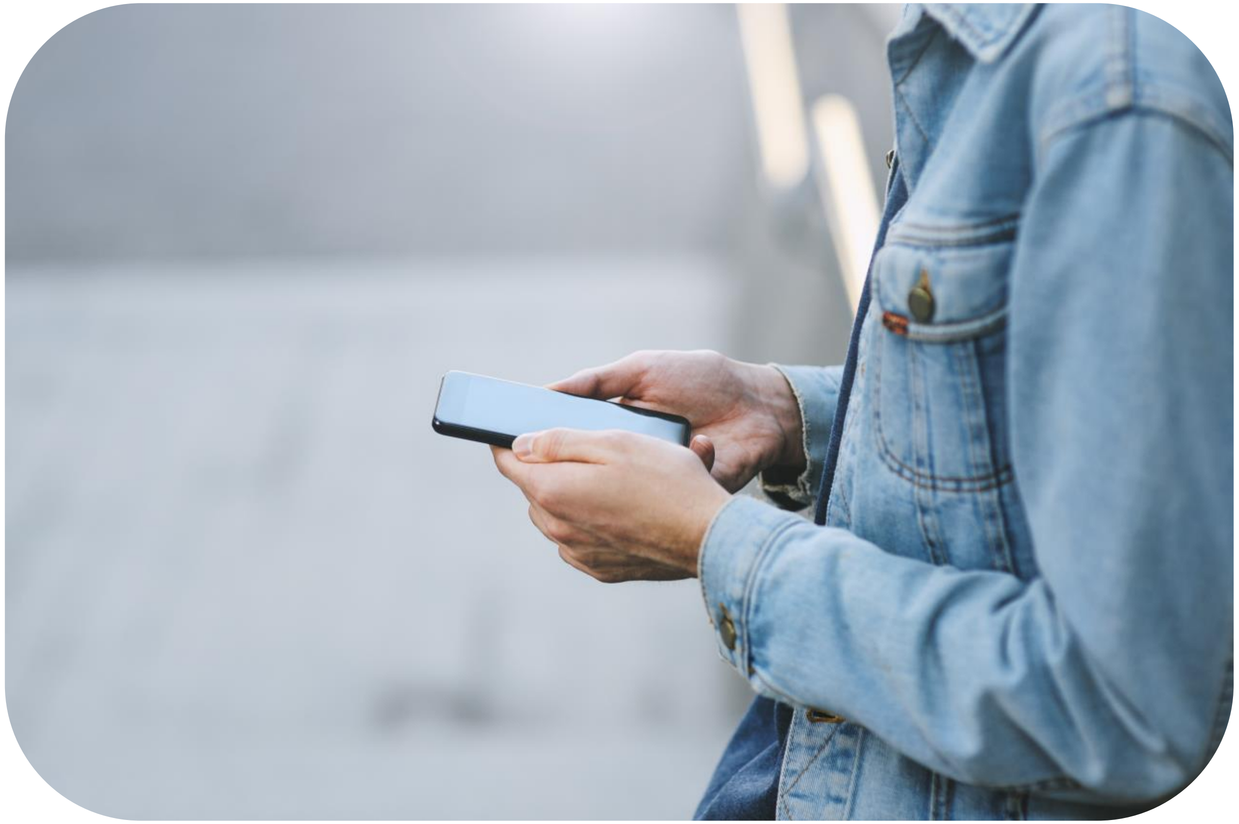
‘Keeping personal data secure’ workbook.

Risks of using public wifi

When connecting to the internet through a public wifi your **online data is at a higher risk of being hacked**.

There are tools available to add another layer of protection to your devices.

Next, we will watch a video on **how easy it is for a hacker to exploit the risks of a public network.**



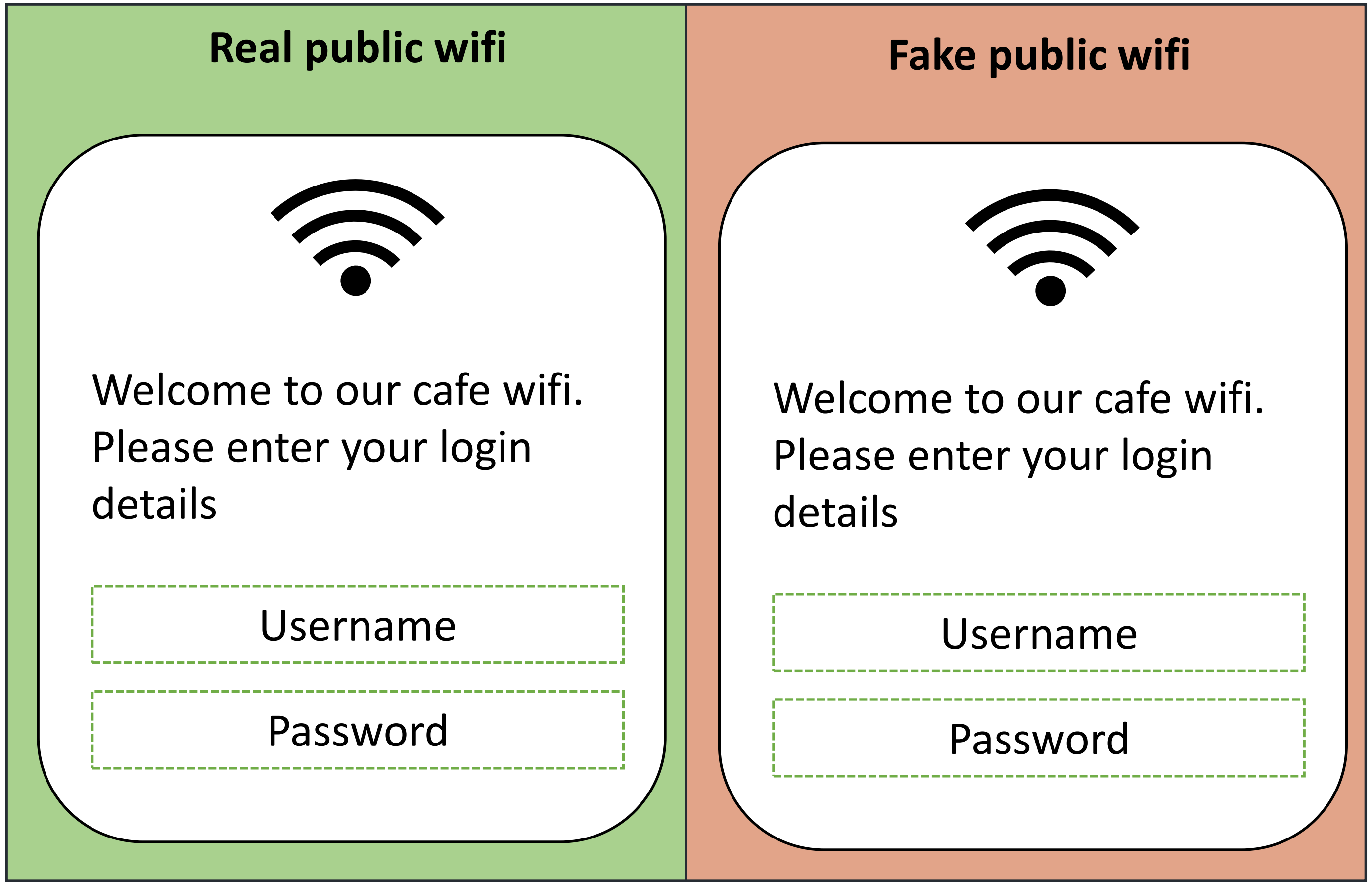
https://www.youtube.com/watch?v=1OVTmrXGHyU&t=13s

How hackers can use public wifi

Hackers can create fake wifi hot spots that look the same as a safe public wifi.

Once you log into the fake public wifi, the hackers can see all information you type into your device, such as

- Usernames,
- Passwords
- Credit card details
- The websites you are visiting



Real public wifi

Welcome to our cafe wifi. Please enter your login details

Username

Password

Fake public wifi

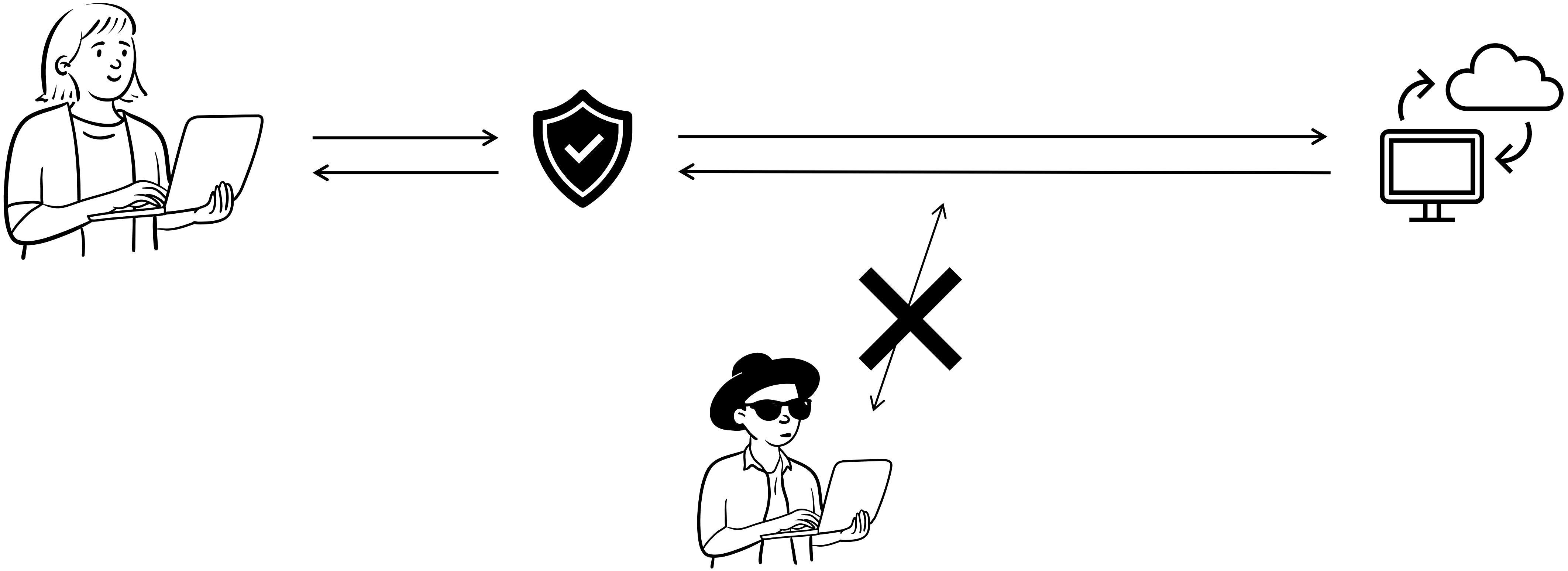
Welcome to our cafe wifi. Please enter your login details

Username

Password

Making public wifi safer

If you need to use public wifi, you can use a tool called a **VPN that encrypts your data** before connecting to the internet.



Definition

Virtual Private Networks (VPN)

Sends information via an encrypted connection to a remote server before accessing the wider internet

Why should you use a VPN?

Prevents loss of sensitive information through eavesdropping

Protects mobile devices that are connected to public wifi hot spots

However they can allow access to blocked applications, which may be illegal

Where can I find a VPN to use?

Some VPN software is free. However, with anything free, care should be taken to ensure there is not a hidden cost in the sharing of user data for example, or limited data usage.

You can sometimes get a VPN with your anti-virus software.

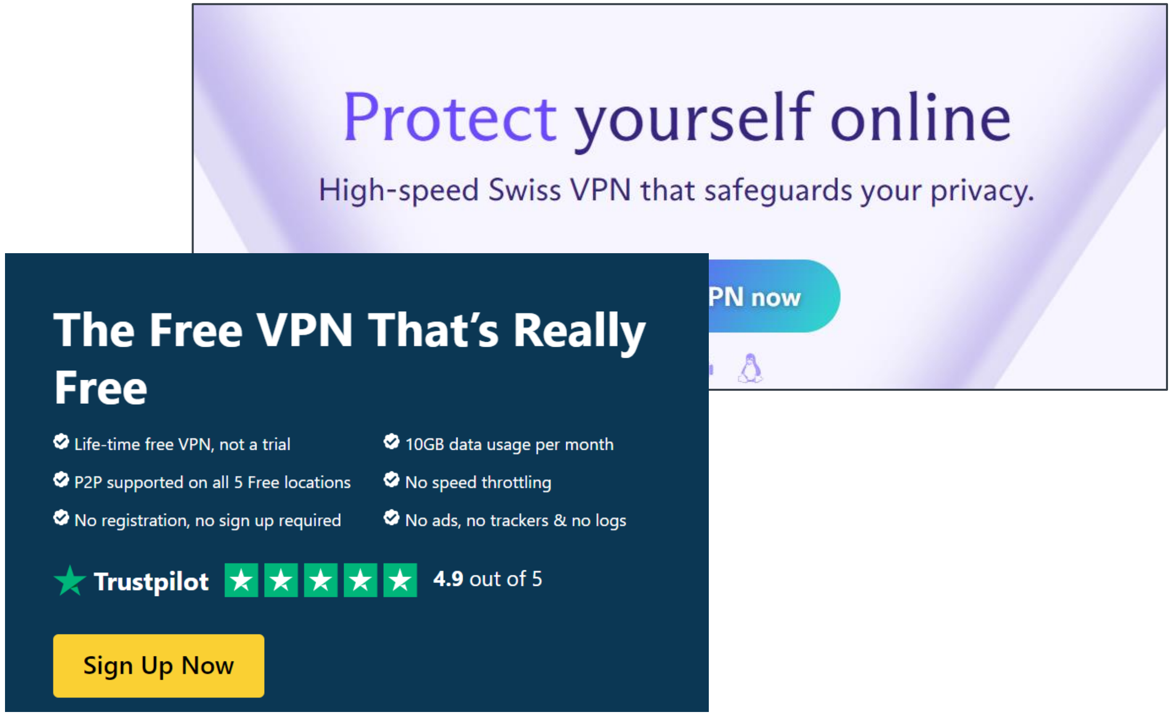
Express VPN

Nord VPN

Proton VPN

hide.me

tunnelbear



Protect yourself online

High-speed Swiss VPN that safeguards your privacy.

The Free VPN That's Really Free

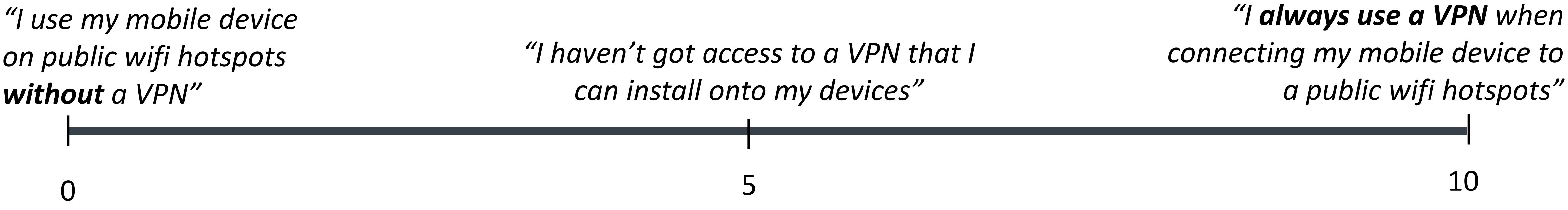
- Life-time free VPN, not a trial
- P2P supported on all 5 Free locations
- No registration, no sign up required
- 10GB data usage per month
- No speed throttling
- No ads, no trackers & no logs

Trustpilot ★★★★★ 4.9 out of 5

Your turn…

Thinking about any mobile devices you use.

On a scale of 0 – 10, do you **use VPN when using your mobile device** on a public wifi network?



*"I use my mobile device on public wifi hotspots **without** a VPN"*

"I haven't got access to a VPN that I can install onto my devices"

*"I **always use a VPN** when connecting my mobile device to a public wifi hotspots"*

Your turn…

You should now have a total “keeping personal data secure” score.

Strong password	7
Password manager	5
Multi-factor authentication	8
Anti-virus	3
Firewall	10
VPN	5
Total score	**38/60**

How safe do you think your personal data is?

Protecting your information online

Even if you have well managed strong passwords and up to date protection on your devices, your personal data can still be visible to criminals.

Information you share on social media, such as photos, location tagging, comments can be used by criminals.

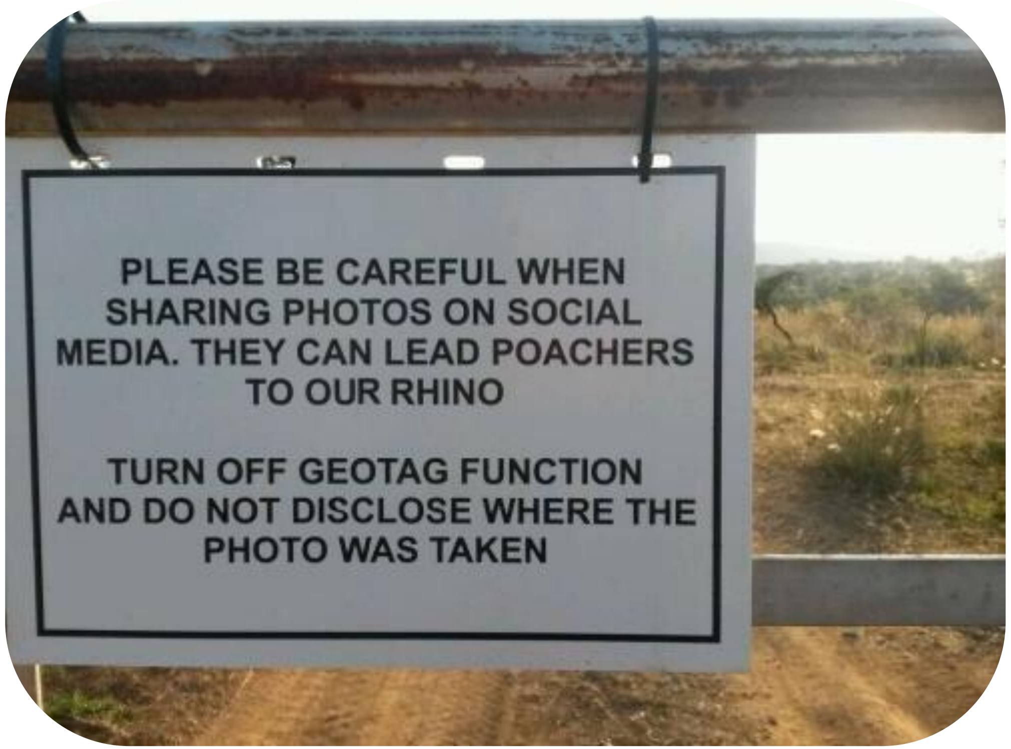
Example

This sign was published on the Reddit page r/ScarySigns.

People were **sharing photos online of the rhinos** that included geotagging or locations.

Poachers are then able to use that information to identify where the rhinos are and hunt them.

Your personal data can be used in ways that you might not expect, which is why you should always **think about what information you are sharing before you post it.**



PLEASE BE CAREFUL WHEN SHARING PHOTOS ON SOCIAL MEDIA. THEY CAN LEAD POACHERS TO OUR RHINO

TURN OFF GEOTAG FUNCTION AND DO NOT DISCLOSE WHERE THE PHOTO WAS TAKEN

https://www.reddit.com/r/ScarySigns/comments/jyxe54/more_than_sad_scary_but_still/

What to think about when sharing data online?

Any data you share can be used. Here are some questions to think about before sharing online your personal details, comments, photos, videos etc.

- **Who can see** the data that I am sharing?
- How could your **data be used**?
- If the photo/video was shared wider, would it be **embarrassing for you** or other people? Remember your data could be online forever.
- Can you **trust the site** you are using? Is it too good to be true?

Next we are going to watch a **video with 5 security tips from a hacker.**

https://www.youtube.com/watch?v=-ni_PWxrsNo

Securing your data check list

There are lots of things **you can do** to keep your data secure. To help you, here is a best practice check list.

- ☑ I have different **strong passwords** for my online accounts
- ☑ I use a **password manager** to store my passwords
- ☑ I have set up **Multi-Factor Authentication** on my online accounts
- ☑ I keep my devices secure with up to date **anti-virus** and **firewall** software
- ☑ I use a **VPN** when connecting to public wifi networks
- ☑ I **think about what I am sharing** before posting online

Next steps

Complete **questions 1 to 4**
in **section 4** of the
‘Keeping personal data secure’ workbook.

Learning checklist

I can *choose and test* a good password.

I can *describe* what a password manager and multi-factor authentication including biometrics.

I can *describe* what is anti-virus software and firewalls.

I can *describe* what a VPN is and know why to use one.

I can *explain* the risks of sharing personal information online.

How you can use this lesson

Created by Effini in partnership with Data Education in Schools and Skills Development Scotland.

Alternative format

If you require this document in an alternative format, such as large print or a coloured background, please contact

hello@effini.com

or

4th Floor, The Bayes Centre
47 Potterrow
Edinburgh
EH8 9BT