

Keeping personal data secure (Answers)



Worksheet section	Contents
1	Personal data & passwords
2	Multi-factor authentication
3	Keeping your device secure
4	Protecting your data online

Version: 1.0

This lesson has been created by Effini in partnership with Data Education in Schools and Skills Development Scotland.

© 2022. This work is licensed under a [CC BY-NC-SA 4.0 license](https://creativecommons.org/licenses/by-nc-sa/4.0/).



You are free to:

Share – copy and redistribute the material in any medium or format

Adapt – remix, transform and build upon the material

Under the following terms:

Attribution — You must give [appropriate credit](#), provide a link to the license, and [indicate if changes were made](#). You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

NonCommercial — You may not use the material for [commercial purposes](#).

ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the [same license](#) as the original.

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**

1. Personal data & Passwords

Reminder

Personal data Information that relates to an identified or identifiable individual

Section 1.1 (recall)

- 1) Which of these pieces of data are personal that would need to be protected?

Data item	Yes/No
Gender	Yes
Telephone number	Yes
WhatsApp message	Yes
Twitter post	No
Your health records	Yes
Newspaper article about you	No

- 2) Fill in the missing words for this definition of a strong password

Combination of letters, numbers and that are difficult to guess by a person or .

Section 1.2 (define)

- 3) Why is securing your personal data important? Please give at least 2 reasons.

1. Prevents your device from being hacked.
2. Stops your data being used for un-ethical reasons
3. Stops fake bank accounts/credit cards being created in your name.

- 4) What is a benefit of using a password manager?

You don't need to remember lots of different, strong passwords. The passwords are secured with a single password.

Section 1.3 (apply)

- 5) Using a password strength testing website such as those below, find out how long these passwords would take it crack.

passwordmonster.com

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

uic.edu/apps/strong-password/

Password	Time to crack
password1	0 secs
\$cotland09	4.72 mins
window.white.heart*	1 year
d\$fl!dfgh&&loc	1 million years
srntyvminsowahh	6,000 years
mypasswordisgood	0.82 secs

Note for teachers:

Answers have been created in passwordmonster.com. Learners may get slightly different answers if they use different websites.

1. Personal data & Passwords

- 6) Using a password generator, create a password that fits with the criteria. Then check how long they would take to crack.

passwordsgenerator.net

lastpass.com/features/password-generator

my.norton.com/extspa/passwordmanager

Criteria	Password	Time to crack
At least 10 characters, mix of numbers and lower case letters	569pwnmye	46 years
At least 12 characters, mix of lower and upper case letters	midsErstonTO	6 months
At least 8 characters, mix of numbers, letters and symbols	XpWv%Dx*	43 centuries
A password you use for an online account (please do not write your password within this workbook)		Depends on the password the learner uses

Section 1.4 (active)

- 7) Thinking about your 'keeping personal data secure' score. What could you do to improve your password related scores?

Area	Your Score	Plan to improve
Strong password		
Password manager		

Note for the teachers:

The answers will depend on the score the learners have given themselves. The answers could cover areas such as using password generator to create strong passwords and using a password manager.

2. Multi-factor authentication

Reminder


Multi-factor authentication Two or more pieces of information are required to gain access to an account

Section 2.1 (recall)

1) Why is it best practise to use multi-factor authentication (MFA) when accessing accounts online?


If your password is stolen or cracked, it will be useless to the criminal without another form of authentication.


2) Which of these can be used to prove your identity when accessing an online account?



Face recognition

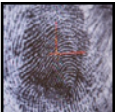
Authentication apps

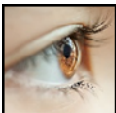




Star sign

Fingerprint





Eye colour

Face recognition,
Authentication apps,
Fingerprint

3) Can you group these ways of proving your identity into, something you know, something you have and something you are?

Email address

Finger print

Use authenticator app

Bank card PIN

Enter code on phone

Password

Something you know

Email address

Bank card PIN

Password

Something you have

Use authenticator app

Enter code on phone

Something you are

Finger print

2. Multi-factor authentication

Section 2.2 (rephase)

- 4) Using biometrics such as fingerprints and facial recognition can be a convenient way of users accessing information, however they are not fool proof. What issues could you come across when using biometrics?

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.

Section 2.3 (active)

- 5) There are many Multi-factor authentication apps available to use. By searching online, find 3 MFA apps that are available and how much they would cost to use.

Name	Cost
Microsoft	Free
Authy	Free
LastPass Authenticator	£0-£3.60/month

- 6) Thinking about an online account you have (e.g Facebook, Twitter), search online to find out how to set up Multi-factor authentication (sometimes called 2-step authentication) for your account and paste a link to the website below.

Online account provider (e.g. Facebook)

Twitter

Link to intructions

<https://help.twitter.com/en/managing-your-account/two-factor-authentication>

- 7) Thinking about your 'keeping personal data secure' score. What could you do to improve your MFA score?

Area	Your Score	Plan to improve
Multi-factor authentication		

Note for the teachers:

The answers will depend on the score the learners have given themselves.
The answers could cover areas such as using one of th MFA apps they have researched.

3. Keeping your device secure

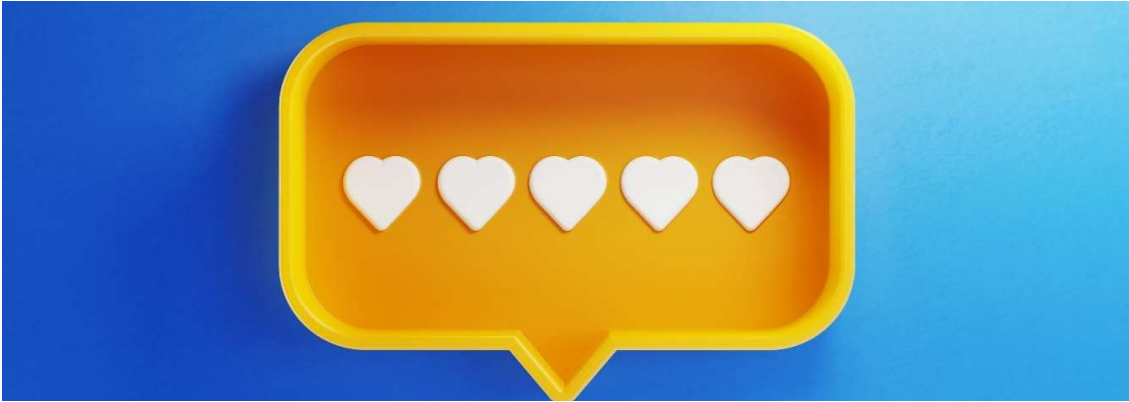
Section 3.1

Below is an article from May 2000, that reports on what is often described as the worst computer virus ever. It was known as the ILOVEYOU worm.

Read over the article, then answer the questions below.

Source: BBC technology website <http://news.bbc.co.uk/1/hi/uk/736080.stm>

'Love Bug' bites UK
Published 4 May 2000



"A computer virus that carries the message "ILOVEYOU" is disabling computer networks across the UK. One estimate says up to 10% of UK businesses have been hit by the bug, which is also being transmitted around the world.

The e-mails have raced across the country, reaching the NHS, universities, City of London institutions, and many large and small companies.

BT, Vodafone, Barclays, Scottish Power and Ford UK were among the giant firms affected.

A spokesman for Lloyds of London insurers said the cost could easily run into tens of millions of pounds in the UK alone.

Even the House of Commons was cut off from electronic communication with the outside world, as the network was shut down to prevent the bug spreading.

It is believed the virus is programmed to delete some computer files, including MP3 music files and images, as well as raiding email addresses to multiply itself and send itself and other e-mails onwards."

- 1) What can you do to reduce the risk of your computer or phone being attacked by malware such as the ILOVEYOU worm in the future?

Have update anti-virus software that runs scans regularly and have your firewalls enabled.

3. Keeping your device secure

Section 3.1

- 2) Ransomware is a type of malware that holds data and computers hostage until a ransom is paid. By searching online, find the names and descriptions of 3 different ransomware virus attacks.

Name	Description
WannaCry	Exploited computers running outdated versions of Microsoft Windows.
AIDS trojan	Dr. Joseph Popp sent infected floppy disks to hundreds of victims.
Bad Rabbit	Spread through a bogus update to Adobe Flash.

Here are some websites might help research ransomware attacks.

<https://www.upguard.com/blog/ransomware-examples>

<https://securityscorecard.com/blog/ten-examples-of-recent-and-impactful-ransomware-attacks>

<https://www.bbc.co.uk/news/technology-56933733>

- 3) There are many providers of anti-virus software available to use. By searching online, find 3 anti-virus software packages that are available and how much they would cost to use.

Name	Cost
AVG	£0
Norton	From £10/year
McFee	From £25/year

- 4) Thinking about your 'keeping personal data secure' score. What could you do to improve these scores?

Area	Your Score	Plan to improve
Anti-virus		
Firewall		

Note for the teachers:

The answers will depend on the score the learners have given themselves. The answers could cover areas such as making sure their anti-virus software is up to date and runs scans regularly.

4. Protecting your data online

Section 4.1 (recall)

- 1) Fill in the missing words for this definition of a VPN

A VPN sends information via an **encrypted** connection to a remote server before accessing the internet.

- 2) What are some benefits of using a VPN?

1. Prevents loss of sensitive information through eavesdropping
2. Protects mobile devices that are connected to public wifi hot spots
3. They can access blocked applications, but this may be illegal

Section 4.2 (rephrase)

- 3) Why does connecting your device to a public wifi hotspot put you at greater risk of being hacked?

Hackers can set up fake public wifi that looks the same as the real wifi. Then when you log on to the fake wifi they can see anything you type into your device such as usernames and passwords.

- 4) You are looking through your social media feed and see this link to a quiz to find out what animal you are most like. What do you need to think about before entering any personal information into this quiz?



Fun Animal Quizzes

Quiz: What animal are you?
Like it, share it and let us know your results!
www.animalquiz.com



The quiz could ask you personal information such name, date of birth, address that could used in ways you would not expect/want.

4. Protecting your data online

Section 4.3 (active)

- 4) Using a search engine such as Google, search for your own name. Did you appear on many websites? Were there any images of you? Were you surprised by what you could see?

Note for teachers: the answer to this question depends on how much they see when the search for their name.