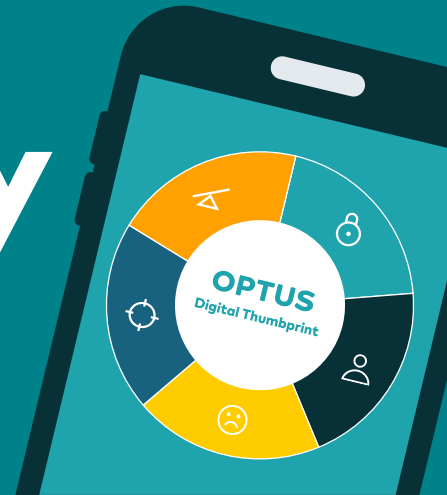


# Protecting your identity

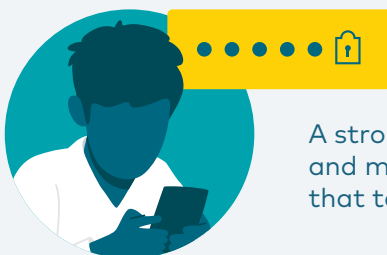
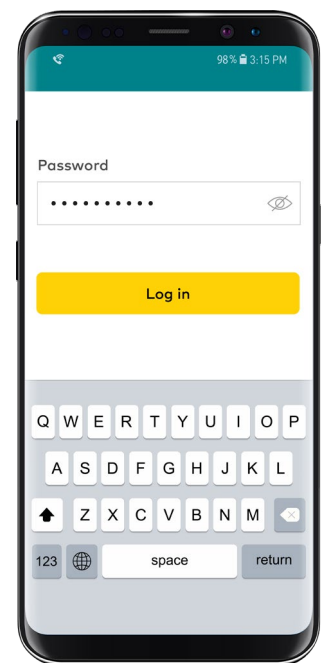
## Passphrases, passwords and MFA



Is your password the same for all your favourite apps and games? Might be your pet's name, your birthday, or your favourite celeb? Or maybe you share your password with your bestie? If you've answered "yes", it's time to level up your online security game and protect your personal information from hackers and scammers.

### This guide will help you:

- ✓ Understand what personal information is and why people want it
- ✓ Create strong passphrases and passwords
- ✓ Learn how to use multi-factor authentication
- ✓ Know what to do if you've been hacked
- ✓ Find more help when you need it

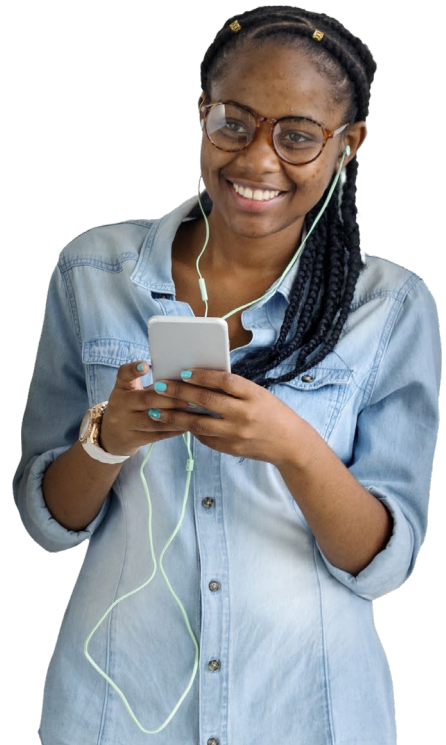


A strong passphrase or password ups your online protection and multi-factor authentication (MFA) adds that extra layer that takes security from good to awesome.

# What is personal information?

Personal information is information about who you are or how to find you.<sup>1</sup> This includes:

- Your full name
- Parents' names
- Date of birth
- Phone number/s
- Home address
- Location check-ins
- Event RSVPs
- School
- Email address
- Photos
- Usernames, passwords or passphrases
- Bank account details



## Why people want your personal information

If someone has this information or hacks your account to steal it they can:



**Pretend to be you**



**Change your posts or profiles**



**Cyberbully or threaten you**



**See or share your private pics and personal information**



**Try to steal your personal identity**

<sup>1</sup> [Protecting your personally identifiable information | eSafety Commissioner](#)

# How to create strong passphrases or passwords

To keep your personal information secure, you need strong passphrases and passwords.

## Strong passphrases

Are more secure<sup>2</sup> than passwords and should be:

### Long

Four or more random words and more than 14 characters

Strong passphrase



M!ntyMilliedonutPickl3paint

### Unpredictable

Not a sentence or popular phrase

Weak passphrase



Happybirthdaytome

### Unique

Different for all your accounts

## Strong passwords

Have a mix of upper-case and lower-case letters, numbers and symbols.

Avoid using these when creating your password:

- ✗ Your name
- ✗ Birthday
- ✗ Pet name
- ✗ Other personal information

Strong password



C9ber5ecurit9!

Weak password



password123



Want to know how long it would take for a computer to crack your password? Test it [here](#).

<sup>2</sup> [Set secure passphrases | Cyber.gov.au](#)



## Keep it secure

- ✓ Change your passphrases and passwords regularly.
- ✓ Keep your passphrases and passwords somewhere safe or, alternatively, use a password manager to store your passwords electronically and securely.
- ✓ Ask a trusted adult to help you to update your device with the latest security downloads.

# How to use multi-factor authentication

Multi-factor authentication (MFA) is a login process that asks you about two or more of the following:



## Something you know

Passwords, answers to secret questions, keystroke patterns, personal identification numbers (PIN)



## Something you have

SMS or email PIN (from authenticator or token-generating apps), ID card, bank card (this might be your parent's)



## Something you are

Fingerprints, face, eyes, voice (biometrics)

## Things to remember:

- × Don't tell your mates your new passphrases, password or MFA info
- × Be careful clicking on emails, links and QR codes saying you've won something – if it seems too good to be true it probably is
- × Avoid "follow" requests from strangers - it could be a bot account, or someone trying to scam you



For details on setting up MFA for your favourite apps, platforms and games, click [here](#).

# What to do if you've been hacked

People who steal passwords and hack accounts are committing a crime. If you think someone has hacked your account or is trying to steal your personal information, tell a parent or trusted adult. You should also let your friends and family know and ask them not to reply to any messages.

## If you can get into your account:

- ✓ Log out of your account on all your devices
- ✓ Change your password
- ✓ Set up MFA
- ✓ Change your account to private so that randoms can't contact you

## If you can't get into your account:

- ✓ Contact social media or game providers to unlock accounts - you can ask a trusted adult to help you
- ✓ Keep any information that might help – date you noticed changes, pics and posts and account names
- ✓ Screenshot any contact or posts if possible



## What to do if you need more help?

If you ever feel anxious, angry or sad about your online security, you should let someone you trust know what's going on. Tell:

- a friend
- a parent
- a teacher
- a trusted adult
- [Kids Helpline](#)

## About Optus Digital Thumbprint

Optus Digital Thumbprint supports digital safety and wellbeing for young people and families. Find out more at [www.digitalthumbprint.com.au](http://www.digitalthumbprint.com.au)

