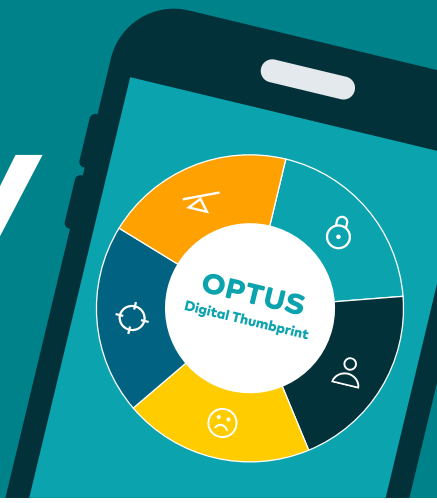
Protecting your identity

Hackers, scammers and fake friends



Have you heard of the three types of cyber criminals? They are the hackers, scammers and fake friends. They live among us online, trying to catch us off-guard to get our personal information. There are many different ways they try to steal your identity but the good news is you have the power to protect yourself! Try out these powerful digital defence skills to stop cyber criminals in their tracks.

This guide will help you:

- ✓ Understand how your personal information is used by cyber criminals
- ✓ Identify different types of cybercrimes
- ✓ Recognise ways to improve your digital defence skills
- ✓ Find more help when you need it

Personal information is information about who you are or how to find you.[1] It is precious and valuable, and cyber criminals online want it for their own gain.

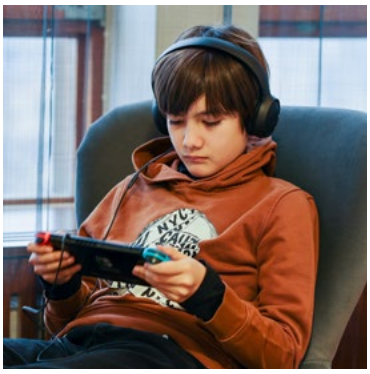
[1] Protecting your personally identifiable information | eSafety Commissioner

Cyber criminals and your personal information

There are three types of cyber criminals you should be aware of.

Hackers may break into your account or devices to get your personal information. Some use a thing called malware.

Fake friends may have bad intentions with using your personal information, even if they are already close with you in real life.



Scammers may trick you into giving them your personal information. Some use malware or phishing links.

Scammers may also look through G.A.P.S to get your personal information:

G Gain trust:

Scammers might say they are from a famous company or impersonate someone you know to make you trust them without thinking too much about it.

A Appeal to your emotions:

Scammers know that you are more likely to help them if you feel bad for them or really like them, so they might lie to you about sick pets or family members, or give you loads of compliments.

P Procedure change:

Scammers will try to send you to websites they have created or phone numbers they have provided you that pretend to be from a bank, gaming platform or other reliable service. It might even feel or look identical to what that site would normally ask you to do.

S Speed:

Scammers create a sense of urgency to get you to make decisions without thinking them through and might say they need money immediately or that you need to act now to get a special deal.

Different crimes by cyber criminals

Once these cyber criminals access your personal information, they can use it in many ways with the help of malware and phishing links/messages. For example:

Catfish

Pretending to be you with your name and photos to trick other people.

Spam

Send out a lot of meaningless or potentially harmful messages using your account.

Dox

Share your personal information to people to scare or harm you.

Identity theft

Use your personal information to steal money or gain other benefits.

Stalk

Threaten, harass and intimidate you online with the personal information they obtained.

Cyberbully

Post mean or embarrassing things about you.

Install malware

A program that steals your personal information, hold your computer or device to ransom and install other programs without your knowledge or consent.[2]

Phish

Steal confidential information, such as online banking logins, credit card details or passwords/passphrases, by sending fake messages (sometimes called 'lures').[3]

[2] Malware | Cyber.gov.au

[3] Phishing - scam emails | Cyber.gov.au

Build your digital defence skills

We've got some simple digital defence moves to fight against hackers, scammers and fake friends. Try to practice all of these moves as much as you can. You can also go through these methods with a trusted adult for extra defence impact.

Digital defence moves:

Speak up

Tell a trusted adult, parent or teacher to form your alliance to defend against cyber criminals.

Get MFA

Use strong passphrases/ passwords and set up multi-factor authentication for your social media or gaming accounts

Check out the Passphrases, passwords and MFA guide here.

Install antivirus

Install antivirus software to protect against malware.

Learn more about malware and what other steps you can take to protect yourself here.

Block randoms

Block or remove followers and accounts that are unwanted.

Check out the Blocking unwanted contact guide here.

Browse securely

Browse websites and webpages that are secure.

A padlock in the address bar or URLs that start with "https" are signs that the website may be more secure. You can often check this before you click on a link, by hovering over the linked text to read where it is trying to send you.

Be scam-aware

Learn about different scams out there to build your scam awareness.

You can go through different scam scenarios in the Scammers and fake friends quiz here.

Update everything

Update apps and devices regularly or turn on auto updates to fix up security weaknesses.

Stay private

Review and enable your privacy settings on your social media and gaming accounts.

Report it

Report and seek help from app and gaming service providers or authorities.

What to do if you need more help?

If you ever feel anxious, angry or sad about hackers, scammers or fake friends, 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

Trusted eSafetyProvider
esafety.gov.au