Online presentation summary

Australian Government

Be Connected
Every Australian online.

Protecting your personal information online

Nearly every app, social media platform or website asks you for at least some personal information. Your personal information includes any details or data that can be used to identify you, such as details locating where you are or where you live, and other unique specific details. It's important to always think twice about sharing personal information.

Protecting your personal information matters

Protecting your personal information is very important as scammers and identity thieves can use it to pretend to be you. They can create fake accounts in your name and act in ways that could impact you now or in the future. This could include fraud, such as stealing money from your bank account or taking out a loan in your name.

Scammers may use your information on its own or in context with other information. It can include everyday things that are specific to you, like your:

Personal information

- Full name
- Home address
- Phone number
- Date of birth
- Driver licence number
- Bank account details
- Email address
- Usernames and passwords

Identity documents

- Driver licence
- Passport
- Birth certificate
- Medicare card
- Australian visa or citizenship certificate
- ImmiCard

Be aware of what you share

Social media

It's a good idea to avoid sharing personal information on your social media accounts. Scammers can learn a lot about you from details you share online. Sometimes they create quizzes or question posts designed to deceive you into sharing personal information. They use this information to guess your account passwords or target you with other scams.

Using apps

Only download apps from the official app stores, and read privacy policies and reviews before downloading anything. You can also limit the information apps have access to. Some apps ask for unnecessary access to your contact lists, camera, storage, location and microphone. Review and adjust your app permissions in the settings menu on your smart device.

Remember: Only accept friend requests from people you know in real life, set your social media accounts to private, and review who can see what you share.

Keep your information secure

Use device security

Using security software on your computer is one of the simplest ways to protect yourself and your privacy. Good computer security includes installing reputable anti-spyware, anti-virus scanners, and firewall software. You should also keep your online security tools and apps up to date by enabling auto-updates. Use automatic and timed screen locks or password-protected screensavers, and have an automatic lockout for multiple login attempt fails.

Tip: A password manager app can also help you to create and store complex passphrases that are hard for others to guess or hack. You can find information on **password managers** and how to set them up on the Be Connected website.

Passphrases

Keep your accounts secure with strong passphrases. Passphrases are the more secure version of passwords and are made up of four or more random words.

Try thinking of a different passphrase for each of your accounts and don't recycle parts of any old ones.

When you choose your passphrase, make it:

- **Long –** at least 14 characters
- **Unpredictable –** use four or more random words with numbers, symbols, and upper and lowercase letters
- **Unique –** don't reuse your passphrases

*E.g. Yellow So Hey Plant > Yell*w-S0heyPl@nt!*

Tip: Check the strength of a password using the NSW Government's password strength tester at **nsw.gov.au/id-support-nsw/be-prepared/passwords**

Multi-factor authentication

It's always a good idea to switch on multi-factor authentication for your accounts. Multi-factor authentication (also known as 2-step authentication) adds an extra layer of security. This means that when you log into an account with your password, you might be asked to do an extra step to confirm that it's you – like enter a code from a text message or use face recognition identification.

Shop securely online

When shopping online, make sure you use trusted sellers and look up customer reviews. Before entering your personal information, check that the website uses 'https' at the beginning of its domain name or has a security icon, usually a small, locked padlock, on its browser to indicate it is a more secure website. When making a purchase, use a secure payment method such as PayPal, BPAY or your credit card.

Use a secure connection

When you need to access important accounts, send sensitive information or enter passwords, connect to a trusted internet connection, such as at home or work, or by using your own mobile data if it's available. Public Wi-Fi is not as secure as your home or work Wi-Fi.

Scams and data breaches

Protect yourself from scams

Being aware of scams and how they work is one of the important steps towards avoiding them. Scammers pretend to be from an organisation or a person you know to try and trick you into handing over your personal information. These are called impersonation scams.

Remember to:

Stop – don't give money or personal information to anyone if unsure
Scammers often ask you to verify who you are or ask you to make a payment.

Think – ask yourself could the message or call be fake?
Beware of unexpected calls, messages and emails. If you are unsure about a message, call the organisation directly using the phone number on their website.

Protect – act quickly if something feels wrong
Contact your bank if you notice some unusual activity or if a scammer gets your money or information.

Tip: Visit the Be Connected website for our free impersonation **scams guide** developed with Scamwatch.

Data breaches

A data breach occurs when personal information held by an organisation is accessed or disclosed without authorisation, or is lost. Many organisations and government agencies have a legal responsibility to tell you if your personal information is involved in a data breach that is likely to cause you serious harm.

If your information is involved in a data breach, make sure you act quickly and get advice provided by the **Office of the Australian Information Commissioner**. The action you take depends on the information involved. Keep a record of what you do. You can also get free support and advice from **IDCARE**.

To find out if a site or app you use has had a data breach you can check services such as **haveibeenpwned.com**. If this has happened, change your passwords straight away.

Identity fraud

If you know or suspect your identity has been stolen:

- Make a report to the Australian Signals Directorate's Australian Cyber Security Centre at **ReportCyber**.
- Contact the police on 131 444. Ask for a police report or reference number as evidence that you made a report.
- If you know or suspect the type of personal information that has been stolen, contact the relevant agency or organisation to let them know.
- Let your financial institution know as soon as possible.
- Make a report to the National Anti-Scam Centre at **Scamwatch** if it was part of a scam.

Take the time to discover Be Connected

Be Connected is a comprehensive website with free resources specifically designed to support older Australians to connect online safely and navigate the digital world confidently. The site is also useful for families and community organisations who want to help older community members access all the benefits of the internet.

Visit beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

This program has been developed by eSafety as part of the Be Connected initiative.