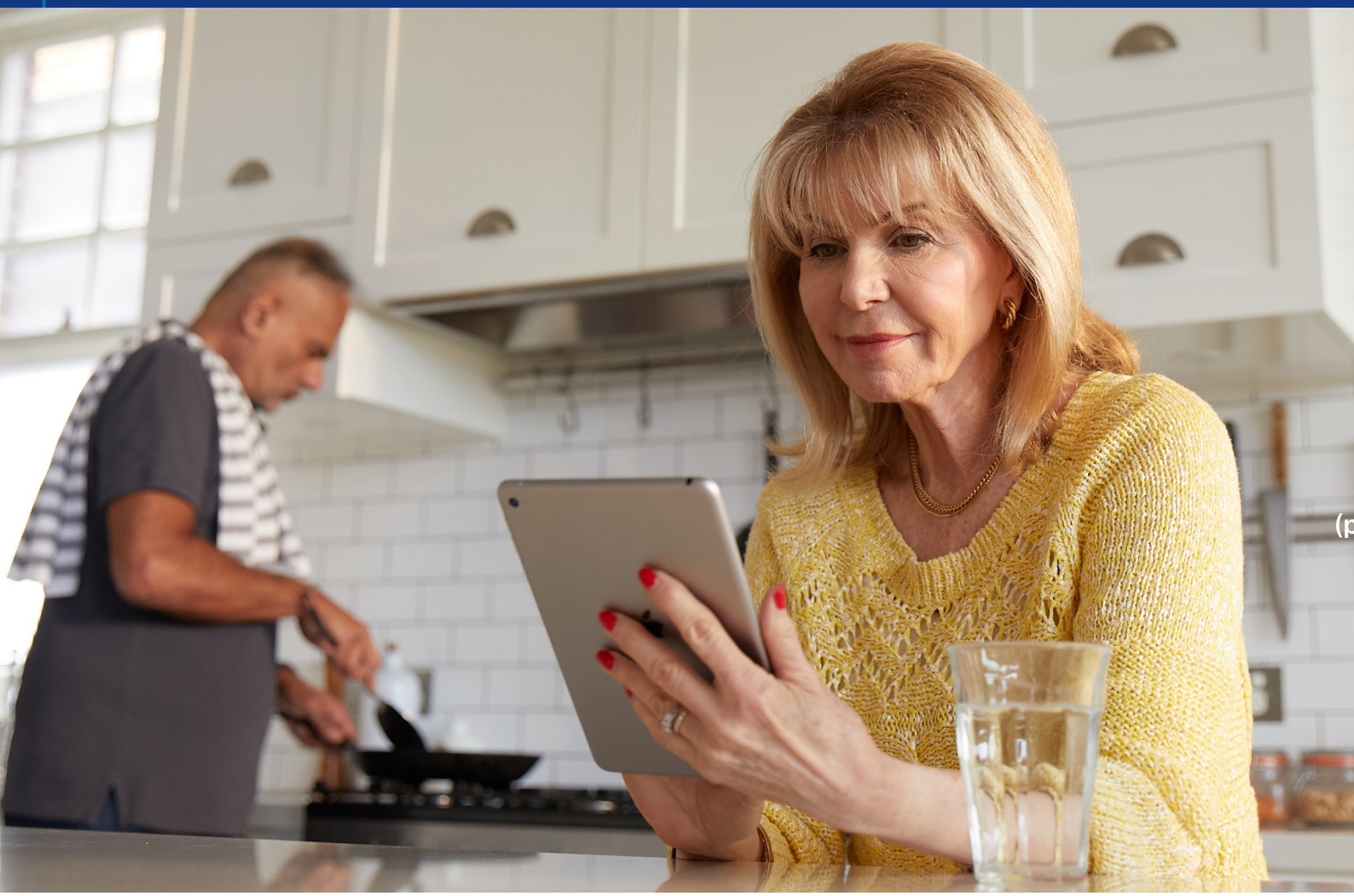
NSW GOVERNMENT

How to protect **your identity** online

Information for seniors



From shopping to banking, paying your bills or keeping in touch with family, we're living more of our lives online. As more services and offerings move to a digital space, it's important that you feel confident and that your identity and accounts are protected.

If your identity documents have been stolen or compromised please contact us on **1800 001 040** or **nsw.gov.au**

ID Support NSW

Password security

- Your passwords should be strong, include letters, numbers and symbols, and be changed regularly.
- Never share your passwords with anyone.
- Instead of writing them down, which is a security risk, consider using an online password manager.
- Don’t use the same passwords for multiple accounts. An online password manager will help with this too (see our ‘common terms’).
- You can also add an extra layer of security by setting up multi-factor authentication (see our ‘common terms’).

Guard your personal information

- Your name, date of birth and contact information are valuable assets and can be used to steal your identity.
- A legitimate organisation will never ask you for your bank details, password, PIN or login details. If you get a call or email asking for any of your personal information – a legitimate organisation will allow you to contact them back through the phone number or email on their website.
- Cyber criminals are clever. You may have seen quizzes on social media asking for your mother’s name, the name of your favourite pet or the first street you lived on – they’re designed to capture your personal information and take control of your online presence.
- Scammers can be extremely friendly and helpful. Be suspicious!

Click carefully

- Over 300 billion phishing emails and 3.5 million phishing texts are sent each day.
- A phishing message (see our ‘common terms’) often has a sense of urgency and asks you to take immediate action.
- Before you click on any links make sure they are from a trusted sender. Do you recognise the email address or phone number? Is the email address spelt correctly?
- Watch out for mistakes in spelling or grammar, or blurry logos.
- If in doubt, delete it.

Visit Scamwatch (www.scamwatch.gov.au) to learn about the latest scams and how to protect yourself.

Protect your devices

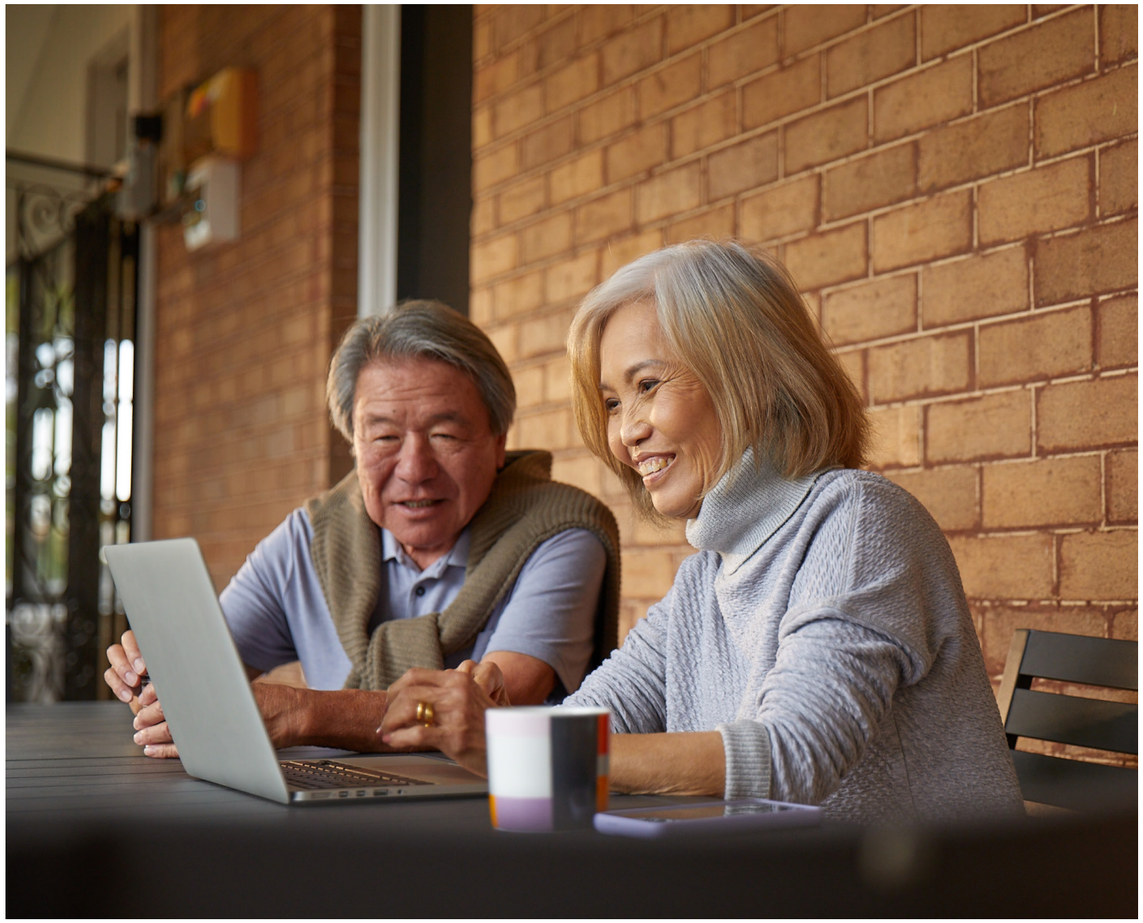
You can keep your devices protected by:

- investing in antivirus software
- updating your operating systems, antivirus software and apps
- setting up strong passwords
- having them lock automatically after a short time
- taking a computer course to increase your knowledge and confidence.

Report a problem

- If you’ve clicked a link that seems suspicious, if you’ve noticed strange transactions in your bank account, or if you stop getting your mail – act immediately.
- Speak with someone you trust, call your bank or alert the relevant organisation. It’s better to notify them – even if you aren’t sure.

It can be upsetting and stressful if your information is compromised – but we’re here to support you. Cybercrime can happen to anyone regardless of where you live, your age or your financial status.



Common tech terms

Term	Meaning
Antivirus software	Antivirus software are programs that protect your devices from becoming infected with viruses.
Cyber criminal	A cyber criminal attacks computer systems with malicious intent. They steal sensitive data about companies or people.
Dark or deep web	The dark or deep web is a part of the internet that's accessed by a special browser that allows users to remain anonymous. It's often used for illegal activity like publishing or buying sensitive information stolen in a cyber attack.
Hacker	A hacker is a computer expert who can gain unauthorised access to computer systems (with or without malicious intent).
Identity crime	Identity crime is when a cyber criminal uses a fake, stolen or manipulated identity to commit a crime. An example is taking out a credit card in someone else's name using stolen identity documents.
Malware	Malware (malicious + software) is a type of software designed to cause damage – to a device, server or network. It can capture personal information, login details and passwords.
Multi-factor authentication (MFA), 2FA or Two-step login	Multi-factor authentication (MFA) is an extra layer of security that uses 2 or more steps to login to a device, account or app. This could be a secret question, a pin number or a single use code.
Online password manager	An online password manager is an app you can install on a device that securely stores your passwords for all your online accounts so you only have to remember a single password.
Phishing	Phishing uses authentic-looking emails to request information from you or to direct you to a fake website. These fake emails try to trick you into downloading malware or sharing personal information.
Virus	A virus is a type of computer program or malicious code that corrupts your devices. Viruses can delete critical files, lock important files so you can't access them or copy your keystrokes to track your login or other information.

DCS_00490