Online presentation summary

Australian Government

Be Connected
Every Australian online.

Shopping and banking online

Shopping and banking online can make your life easier, providing you with modern conveniences while helping you avoid queues and save time. You can buy items, transfer money and pay bills from a computer or your mobile device, giving you choice and freedom whether you're at home or out and about. Follow our safety tips on shopping and banking online and enjoy the many benefits that the internet can provide.

Shopping online

Millions of Australians are choosing to shop online, and there are many reasons why:

- it can save you time and provides the convenience of being able to shop anywhere 24/7
- it's easy to research items and compare prices
- you can access a wider range of products that may not be available in store
- reviews help with making an informed decision.

While online shopping provides many benefits, it pays to be cautious!

Use secure websites and payment services

Before you enter personal or payment details online, check how secure the website is. Look for:

- a padlock beside a website address in the address bar or a URL that starts with 'https' instead of 'http'. This can mean a site is more secure than other sites
- trust marks or seals that show the site has met security and privacy requirements (for example 'McAfee secure' or 'Norton').

When making online payments, only pay for items using a secure payment method like PayPal, BPay or your credit card. Using credit cards can minimise risk when shopping online because they offer extra protection and make it easier to get your money back if anything goes wrong.

Never pay by direct bank deposits, money transfers or other methods (Bitcoin).

Remember: No matter how you pay, be sure to keep your purchase confirmation emails and check your bank statements to see that you've been charged the right amount.

Use trusted sellers

Research online shopping websites before you buy and stick to well-known, trusted retailers. Search for reviews from other customers and find out where the online store is based. While overseas retailers need to comply with Australian Consumer Law, some make it difficult to return items. If it is an Australian retailer, you are in a much better position to sort out the problem if something goes wrong.

Read the terms and conditions

Before you buy, read the fine print including warranty, refund, complaints and handling. Familiarise yourself with the retailer's cancellation and returns policy and find out key information you may need like who pays for the return shipping, do you get a full refund or store credit and how long is the return period. This information is usually found at the bottom of the webpage.

Be alert to online shopping scams

Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site. Keep in mind that scammers:

- often only accept payment in the form of money order, wire transfer, international funds transfer, pre-loaded card or electronic currency, like Bitcoin
- don't provide contact details or have limited information about delivery and other policies
- are often selling goods at prices that are too good to be true
- are often a very new online store with very few reviews
- often have poor reviews.

The best way to detect a fake trader or social media online shopping scam is to search for reviews before purchasing.

Banking online

Some Australians still go into a branch to do their banking, but internet banking is becoming more popular. It's easy to see why when banking online can:

- save you time because there's no need to travel or wait in long queues
- make it convenient to check your balance, access your account and pay bills any time of the day or week
- save you money with suppliers who provide a discount for direct debit payments
- keep a record of all the bills you have paid online for easy reference
- put you in full control of your accounts, allowing you to make all the transactions yourself and view up-to-the minute information.

Banks have sophisticated security systems to make sure your money is secure when banking online, but there are still things that you can do to help keep your money safe.

Create unique strong passwords

Use strong passwords to make it harder for other people to guess them and access your personal information. It should not be a recognisable word, and it should have a minimum of 12 characters, with a mix of numbers, upper and lowercase letters and symbols. Do not use the same password for everything and remember to change your passwords regularly. Don't allow your web browser to store your username and password for banking.

Tip: Take a phrase, song lyric, or passage from a book or poem you enjoy. For example, the 1960s song You Can't Always Get What You Want by the Rolling Stones could help create a password that is memorable to you, like: ycagwyw. To make the password stronger, you can capitalise some of the letters, add some numbers and special characters or punctuation.

For example, by capitalising the first and last letter, adding the decade the song was released and a special character you could end up with: 6YcagwyW60$*. This is a much stronger password that is still memorable to you.

Be careful not to use anything else that could be easy for others to guess, like your birthday.

Enable multi-factor authentication

Multi-factor authentication or MFA, sometimes referred to as two-factor authentication or 2FA, provides you with an extra level of security on your account. It helps protect your account by requiring your username and password, plus at least one extra security check that only you can access such as a security code. For example, your bank might send a secret security code to your mobile phone. You need to use the code to authorise what you're doing in your online banking session, such as making a payment.

Only bank on a secure site

As with online shopping, look for the 'https' at the beginning of the address bar which indicates you are visiting a more secure page, and always log out of your account when you are finished. Also, avoid using a public computer or public Wi-Fi to do your banking online.

Make sure your device is up to date

Use antivirus software such as McAfee or Norton. Turn on automatic updates for operating systems and applications (such as web browsers). New versions of operating systems and applications usually have new security features.

Beware of scammers

Phishing scams are used to steal your money by tricking you into revealing personal information such as your bank account or credit card details, and usernames and passwords. Your bank will never ask you to 'confirm' or 'verify' your details by text or email. If you receive an official looking message from a bank, government agency or business, never use the contact details in the message. Contact them directly by doing an internet search for their phone number or email address.

Tips for using public Wi-Fi safely

You should never use public computers or public Wi-Fi networks for online banking, making payments online or to complete a form that requires you to enter personal details. The computers and Wi-Fi networks you can use in some libraries, airports and other public areas may not be secure, and there may be a chance that someone sees your personal financial information or your logon details.

Free public Wi-Fi can be used to access the internet and catch up on the news, or to do things that don't require you to enter your personal details.

There's help when you need it

When things don't go as planned online, there's always somebody you can talk to.

Online shopping:

1. First, contact the online seller or website.
2. If you can't resolve your problem directly with the online retailer, your local state or territory consumer protection agency (sometimes called 'consumer affairs' or 'fair trading') can provide you with information about your rights and options. They may also be able to help negotiate a resolution between you and the seller.
3. If you suspect you have been scammed:
   - Contact your bank or financial institution immediately to stop any further payments to the scammer.
   - If you have experienced cybercrime and lost money online, you can report it to the police via ReportCyber or visit: cyber.gov.au
   - If you are concerned that your personal information has been exposed and misused, contact Australia's National Identity and Cyber Support Service IDCARE on 1300 432 273 or idcare.org
   - Report the scam to the Australian Competition and Consumer Commission (ACCC) at scamwatch.gov.au/report-a-scam. This helps to warn people about current scams, monitor trends and disrupt scams where possible.

Tip: the ACCC has a complaint letter tool you can use to help you draft a letter or email to the seller.

Online banking:

Contact your bank or financial institution immediately if you notice any unusual charges, withdrawals or other activity on your account.

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.