FAMILIES OF VETERANS GUILD

SAFE ONLINE SHOPPING AND BANKING

Tips for secure transactions and trusted websites

Shopping and banking online can be convenient and time-saving—but it's important to know how to do it safely.

Scammers often target older Australians with fake websites, emails or messages, especially those pretending to be from banks or well-known retailers.

This guide offers practical tips to help you shop and bank online securely, based on advice from the Australian Cyber Security Centre (ACSC), eSafety Commissioner, and the Scamwatch program from the Australian Competition & Consumer Commission (ACCC).

Shopping online safely

1. Shop only from trusted websites

- Stick to well-known retailers or those recommended by people you trust.
- Look for web addresses that start with https:// (the "s" stands for secure) and a padlock symbol next to the address bar.
- Avoid clicking on links in emails or ads—go directly to the store's website by typing the address yourself.

2. Be cautious of "too good to be true" deals

- Scammers often lure people with heavily discounted products or fake giveaways.
- If the price is unusually low or requires payment by gift card, crypto or direct deposit—it may be a scam.

3. Check reviews and contact details

- Look for reviews from real customers and check if the business has a physical address and phone number.
- If something feels off or hard to verify, it's best to avoid the purchase.

4. Use secure payment methods

- Credit cards and services like PayPal offer extra protections in case something goes wrong.
- Avoid direct bank transfers unless you are sure the seller is legitimate.

Banking online safely

1. Use strong and unique passwords

- Create different passwords for each account and make them hard to guess. A good tip is to use a memorable phrase with numbers or symbols.
- Consider using a password manager or writing down passwords and storing them safely (not on your device).

2. Turn on two-factor authentication (2FA)

- Most banks offer 2FA—this is a second layer of security where you get a text message code or use a secure app when logging in.
- This helps protect your account even if someone learns your password.

3. Be alert to fake emails and texts (phishing scams)

- Banks will never ask for your PIN, password, or account details via email or text.
- If you're unsure, call your bank directly using the number on the back of your card—not one in the message.

4. Log out and close your browser

- After online banking, always log out and close the browser window—especially on shared devices.

More tips

- **Keep your devices updated:** Install software updates when prompted—they often include important security fixes.
- **Use antivirus software:** A good security program can protect your device from malware and phishing attempts.
- **Never save payment details on shared devices:** This can expose you to fraud if others use the same computer or tablet.

Where to get help

If you think you've been scammed or need support:

- **Scamwatch: www.scamwatch.gov.au – Report scams and find updates.**
- **Your bank's fraud team – Contact them immediately if you suspect fraud.**
- **IDCARE: www.idcare.org – Free support for identity and cyber issues.**
- **eSafety Commissioner: www.esafety.gov.au – Digital safety resources for Australians.**

About this sheet

This information sheet was created using guidance from the Australian Cyber Security Centre (cyber.gov.au), the eSafety Commissioner (esafety.gov.au), and Scamwatch (scamwatch.gov.au). These are official, government-backed resources providing reliable and up-to-date information about online safety in Australia. Scan the QR code to learn more about online safety.