Tech Savvy Seniors

Module 6: Stay safe online and avoid scams

I can:

- ❑ Describe common types of online and phone scams.
- ❑ Identify scam red flags in email, SMS, phone calls and websites.
- ❑ Take steps to protect personal information.
- ❑ Block, delete, or report a suspected scam.
- ❑ Understand where to go for help and support.

Key takeaways

My key insights from today are:

Support

I can get support from:

My action plan

In the next week, I will:

1

2

3

My notes

Tech Savvy Seniors

Module 6: Stay safe online and avoid scams

What are scams?

- Scammers pretend to be someone they're not — like your bank, the government, or a phone company — to get you to trust them and trick you into giving away your money, personal details, or access to your devices.
- They might use email, text messages (SMS), phone calls (real people or robocalls), pop-up messages on websites, messaging apps or social media.

What are scammers after?

- Bank or credit card numbers
- Personal information (name, date of birth, address, Medicare number)
- Passwords
- Access to your computer or phone
- Money via transfers or gift cards
- Your contact list (to scam others in your name)

How to protect yourself

- Create strong passwords:
  - Use a mix of capital and lowercase letters, numbers and symbols (e.g. Happy$Fish24!)
  - Avoid using the same password on multiple sites
  - Never share your passwords unless with someone you fully trust (e.g. a carer
  - Turn on 2-factor authentication (2FA) when it's available.
- Lock your device when not in use
- Update your software regularly

Safe actions

1. **Stop –** Don't rush. Scammers want you to act quickly. Always take a moment before clicking or giving your money or personal information to anyone.
2. **Check –** Make sure the person or organisation you're dealing with is real. Contact the organisation directly using phone numbers or email addresses you find on their official website or app.
   Look for red flags:
   - Urgency – "Act now", "urgent"
   - Fear – "You've been hacked"
   - Temptation – "You've won a prize"
   - Unfamiliar sender or number
   - Poor grammar or spelling
   - Strange links
   - Requests for personal info
3. **Protect –** Act quickly if something feels wrong. The sooner you act, the better you can protect yourself and others from scammers.
   - Contact your bank if you think you've lost money or shared financial details.
   - Contact IDCARE (www.idcare.org or call 1800 595 160) if you want support.
   - Report to Scamwatch (www.scamwatch.gov.au) to protect others.
   - Report to police (www.cyber.gov.au).
   - Change passwords and security details if you think they've been compromised.
   - Monitor your bank statements and credit reports for unusual activity.
   - Report the scam to the impersonated organisation.
   - Being scammed can feel overwhelming. Support is available at Lifeline on 13 11 14 or Beyond Blue on 1300 22 4636.

Source: Scamwatch's Stop, Check, Protect method

User guide

Scan the QR codes (with your camera) or click the links.

BeConnected
Identifying and avoiding scams

NSW Gov
Tips to staying safe online

Scamwatch

Cyber.gov.au
How to dispose of your device securely

NSW GOVERNMENT