eSafety with Be Connected

More than ever, older Australians are getting online to enjoy the benefits the internet has to offer, whether it's connecting with family and friends, doing online banking, buying or selling, researching travel or socialising. Did you know there are 2.8 million active Facebook users in Australia aged over 55*?

Scams

It's fantastic that older Australians are engaging online and empowering themselves in the digital age. However, the internet is not without its own risks, so it pays to be savvy and safe online.

On the internet, we cannot always be sure that people are who they say they are. Being aware of internet tricksters is one of the most important steps towards avoiding them. Once you know their tricks, you should be able to easily spot a scam when you see one.

Romance and dating scams

Unfortunately, scammers often take advantage of older Australians who have recently divorced or lost a partner. They trawl through social media and dating sites to target people who may be in emotionally vulnerable states.

Dating scammers will create fake online profiles to make contact (also known as 'catfishing'). They will befriend or show romantic interest in you then ask for 'gifts' or money, so it's important to keep your wits about you.

What can you do to be savvy and safe?

Look out for:

- People that express deep affections for you very quickly, but then ask for help with medical and other expenses.
- People who avoid meeting face to face and make up excuses as to why they can't travel to see you.
- People whose profile on the dating site is inconsistent with what they tell you.

Don't:

- Transfer any money to somebody you've only spoken to by phone or email.
- Send personal information such as your date of birth, bank or credit card details.

How to check if someone is real or not:

- Run a google image search to see whether their image matches who they say they are or if it's stolen from someone else. Ask someone to help you do this if needed.

Unexpected prize & lottery scams

With these scams, you'll receive a message saying that you have won a prize or lottery but in order to claim your prize, you will need to pay an upfront fee. The prize could be anything from a tropical holiday to cash or a smartphone.

What can you do to be savvy and safe?

Look out for:

- Messages asking you to pay a fee in order to receive your 'prize'. Legitimate sweepstakes will never ask you to pay fees to participate in, or receive, a prize.
- Messages or people that pressure you to act quickly otherwise you'll lose your 'win'.
- Messages asking for your bank or credit card details to receive your prize.
- Competitions or lotteries you've never entered telling you that you have won something.

Don't:

- Respond to competitions you haven't entered.
- Provide your bank or credit card details.

Remember: if you haven't entered a lottery or competition, you can't win it.

Tech support scams

These scams usually start with a call or email from a large, well known organisation to tell you that you have a computer or internet problem and they can fix it. The caller will request remote access to your computer to find out what the problem is and try to convince you to download or buy software to fix the problem.

What can you do to be savvy and safe?

Look out for:

- THEY called YOU. Large organisations expect you to call them when you have a problem with your internet or computer - they will not call you.
- They ask you to buy software or sign up to a service to fix the computer.

What should you do if you get a call like this?

Hang up!

Don't:

- Provide remote access to your computer.
- Provide them with personal information such as your bank account or credit card details.
- Buy software from an unsolicited call or email.

Phishing scams

'Phishing' scams are the most common form of scam on the internet. They usually start with an email, text message or phone call that seems to be from a trusted business like a bank, telephone or internet service provider, asking you to 'confirm' your account details. By confirming your details, you're actually providing them to the scammer.

What can you do to be savvy and safe?

Look out for:

- Emails, text messages or phone calls that ask you to verify, update or re-enter your personal details such as your bank account, credit card number or username and password.
- Urgent emails or text messages telling you something unusual is occurring with your account or it's being suspended and you need to click on the link to rectify it.

Don't:

- Click on any links - just press delete.
- Open any attachments as they may download a computer virus.
- Use the contact details provided in the message, they could be fake.

If you're still unsure about the message you've received, do an internet search for the company it appears to be sent from and contact them directly.

Help, I suspect I'm being scammed

If you think you've been the victim of a scam, don't be embarrassed and don't keep it to yourself. There are steps you can take to fix the problem:

- Contact your bank and stop any further payments to the scammer.
- Report the scam to the ACCC (Australian Competition and Consumer Commission). Head to scamwatch.gov.au for help with reporting and understanding scams.
- Raise awareness. If there's anybody else you know who might be a victim, let them know.

Remember:

There's always someone who can help – whether it's the anti-scam folks at the ACCC, a technically-minded friend or family member, or even a local computer club.

Scams are intended to take advantage of your good nature, but if you're careful about sharing personal information online, use common sense about who you send money to, and keep your guard up, the internet can be a safe place to explore.

Safety first on Be Connected

You can learn more about other safety topics on the Be Connected site: beconnected.esafety.gov.au. The 'Safety first' course will teach you the essential skills to stay safe online, as well as the 'why' and 'how' of safe passwords, paying for goods safely online, and how to download and save files from the internet safely.

*Source: Cowling, D. (1 February 2018). Social Media Statistics Australia - January 2018. Available at Socialmedianews.com.au. Accessed 20 April 2018.