# Now&Next

WINTER **2023**
ISSUE **15**

## How to stay cyber safe

Count
The confidence to look ahead

# How to stay cyber safe

**Cybercriminals and fraudsters are constantly finding new and creative ways to scam us. Here are some of the most common cyber scams – and the surprisingly straightforward ways to protect yourself against them.**

If you've received a communication from a scammer this year, you're certainly not alone. The Australian Bureau of Statistics reported in February 2023 that scammers tried conning 65% of Australians aged over 15 in the 2021-22 financial year.[20] And small businesses across Australia lost almost $13.7 million to frauds including false billing scams and payment redirections in 2022, says the Australian Competition & Consumer Commission (ACCC).[21]

With scammers and hackers only getting more sophisticated in their trickery, it's vital to be prepared. Here are the most common cyber scams and how to guard against them.

## An investment offer too good to be true

Investment scams cost Australians $1.5 billion in 2022.[22] Be wary if someone calls you with an investment offer of a lifetime or the chance to buy the next big digital currency – but says you need to invest right now or you could miss out. Hang up immediately.

## Strange emails and text messages

Scammers send emails and text messages to try and trick you into revealing information such as passwords, account and identification details or credit card numbers. They may also try to manipulate you into downloading malware onto your mobile phone or computer that tracks your online activity to steal your passwords or login details.

A scammer can impersonate a trusted organisation, such as Microsoft, a bank, superannuation fund, insurance company or government agency. Using the organisation's logo, the scammer tries to trick a victim into opening an email, instant message or text message.

Be suspicious if an email has misspellings. Another red flag is when the sender's email address doesn't seem right. And whatever you do, don't click the links!

## Mystery phone calls

Related to email and text message scams, these types of scams involve a phone call (or a voice message) from someone claiming to be from the tax office or another government agency. They threaten you with arrest, legal action or other demands to pressure you into handing over your money or personal details. If you get a call like this, simply hang up and report it to the relevant government agency. If you're uncertain whether the call is genuine, hang up and call the organisation using their official phone number.

## The best defence

Staying vigilant and informed is your best defence against scammers. In fact, the only good thing about their increased prevalence is that more of us now know about their methods.

The ABS says that fewer people (2.7%) responded to scams in 2021-22 than the previous financial year (3.6%).[23] Of those who do, more of them are contacting relevant authorities[24] such as their bank or the police.

## Top tips for staying cyber safe

- Use multi-factor authentication where possible, including for your email and social media accounts.
- Never give out personal or security-related information via phone, email or text message. This includes your superannuation or insurance policy numbers, online passwords, card details or security codes.
- Pause before sending money. If you receive a request for payment that doesn't seem right, phone the person who asked for the payment to check if the request is from them and confirm the details.
- Don't click on links or attachments in text messages or emails.
- Use strong, long and unique passwords for each account, and change your passwords at least every year. That way, if a scammer uncovers one of your old passwords, you'll be protected. Don't use the same password across social media, email, superannuation, insurance and banking accounts.
- Keep your devices up to date as cybercriminals target security holes in outdated software. So, make sure all your devices, operating systems, security software and applications are current and set to auto-update.
- Secure your physical mail with a locked letterbox or a PO Box and report any missing mail to relevant providers. Don't throw away financial documents or bills in the rubbish or recycling bin. These often contain personal and financial information. Shred them or have them securely destroyed. Consider receiving your bill and account statements online.
- Don't post anything on social media that may reveal sensitive information about you, your friends or your family. Regularly check your privacy settings and be wary of sharing personal information with online quizzes.
- Get investment recommendations from your financial adviser, not a scammer. If an investment sounds too good to be true – it's probably a scam.

20 https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams

21 Targeting scams 2022.pdf (accc.gov.au) p7 Heading 1.5 bullet point 2

22 Targeting scams 2022.pdf (accc.gov.au) p. 10 Table 2.2. Total column.

23 https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams

24 https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams

Be suspicious if an email has misspellings. Another red flag is when the sender's email address doesn't seem right. And whatever you do, don't click the links!

## How we can help

Jeopardising your cyber safety can cost you more than money. It can also unsettle your peace of mind. Speak
to us if something doesn't seem right so we can discuss the best course of action.