

Scamwatch

Scamwatch is a website run by the Australian Competition and Consumer Commission (ACCC). It provides information to consumers and small businesses about how to recognise, avoid and report scams.

You can find the Scamwatch website either by searching for 'scamwatch' using your favourite browser or by clicking on the link here: <https://www.scamwatch.gov.au/>

The ACCC has launched a podcast series for this year's National Scams Awareness Week to provide Australians with tips on how to protect their personal and financial details from scammers.

The five-episode podcast series, *This is Not Your Life*, is produced by Julian Morrow, the creator of ABC TV's consumer series *The Checkout*. The podcast, which is a parody on the popular TV show *This Is Your Life*, contains advice on how to avoid a scammer stealing your identity and features cameos from ACCC Chair Rod Sims, eSafety Commissioner Julie Inman Grant and IDCARE's founder David Lacey.

Scamwatch has received a staggering 24,000 reports of stolen personal information this year alone, an increase of 55 per cent compared with the same time last year.

Australians reported losing more than \$22 million to scammers who also stole their personal information and people aged 25–34 reported losing personal information more than any other age group.

Scammers are targeting personal information more than ever which has contributed to an increase in financial losses across all scams, up to \$91 million so far this year.

This year's National Scams Awareness Week (17–21 August) has over 100 partners from the government, NGO and business sectors working together to raise awareness about scams that steal personal information under the tagline: 'Be yourself. Don't let a scammer be you'.

"During the COVID-19 pandemic, with more people working and socialising online, we have unfortunately seen a sharp increase in scammers seeking personal information," ACCC Deputy Chair Delia Rickard said.

"Personal information, such as bank and superannuation details or passwords, are extremely valuable and scammers will try to steal them for their own financial gain. Our increased use of technology has created more opportunities for them to do so."

"Scammers will also try and steal a range of other documents, or the numbers associated with them, including passports, driver licences, credit cards, tax statements, utility bills or Medicare cards, so that they can impersonate you," Ms Rickard said.

Phishing scams, the most common form of scam, are up by 44 per cent compared with the same time last year. Scammers pretend to be from government departments and

businesses, like the ATO, myGov, Telstra or the NBN, to gain bank account details and other information about a person that can be used to impersonate them.

Once a scammer has that information, they can then use it to access individuals' bank accounts or superannuation, take out loans under their names and impersonate them on social media to try to get money from family and friends.

“Scam victims who have lost personal information are vulnerable to further scams, fraud or identity theft,” Ms Rickard said.

“If you do have your identity stolen, it can take years to recover and people can end up losing more than money. Not only time in trying to undo the damage done financially, but it can also impact greatly on your mental health.”

“Never give your personal or financial information to anyone you don't know or trust via email, text, social media or over the phone,” Ms Rickard said.

Background

If you suspect you are a victim of identity theft, contact IDCARE on 1300 432 273. IDCARE is a free government-funded service which will work with you to develop a specific response plan to your situation and support you throughout the process.

If you have been the victim of a scam, contact your bank as soon as possible and contact the platform on which you were scammed to inform them of the circumstances.

More information on scams is available on the Scamwatch website, including how to make a report and where to get help.

Alternatively, you can click on the links below to access the podcasts:

[Trailer](#)

[Episode one: Phishing scams](#)

This is Not Your Life 'celebrates' the career of a master of the phishing scams designed to trick you into disclosing the surprisingly small amount of personal information that scammers need to steal your whole identity.

[Episode two: Online shopping and classified scams](#)

This episode lures a master of online shopping and classified scams into the studio to reveal the tricks of her (criminal) trade ... information you can use to protect yourself when shopping online

[Episode three: Romance scams](#)

Love is in the air on the next episode ... but not true love. This is Not Your Life 'celebrates' the career of a master romance scammer and reveals the tricks romance scammers use to turn fake love into real money.

[Episode four: Business email compromise scams](#)

In this episode of This is Not Your Life, meet a master of business identity theft who sends out bogus invoices from real businesses ... hoping to trick you into paying into the scammer's account. Plus learn how to avoid installing malware on your computer at work or home

[Episode five: Remote access scams](#)

Lock up your laptops because on the final 'special COVID-19 lockdown' episode of This is Not Your Life for Scams Awareness Week 2020 we feature the scammer who cons you into letting her access your computer remotely.