



ACCC AUSTRALIAN
COMPETITION
& CONSUMER
COMMISSION



Scamwatch radar alert

How criminals steal your identity information to steal your money

Dear radar subscriber,

Scams reported to the ACCC involving identity theft or the loss of personal/banking information have cost Australians at least \$16 million this year, and this figure is likely to be just the tip of the iceberg.

Four in 10 [Scamwatch](#) reports in 2019 involve attempts to gain information or the actual loss of victims' information.

“If you think scammers might have gained access to your personal information, even in a scam completely unrelated to your finances, immediately contact your bank,” ACCC Deputy Chair Delia Rickard said.

“Timeliness in alerting your financial institution is absolutely crucial, and will give you the best

possible chance at recovering your funds.”

Some of the ways scammers obtain personal or banking information are:

- phishing emails and text messages which impersonate banks or utility providers seeking your login details
- fake online quizzes and surveys
- fake job advertisements
- remote access scams in which the scammer has direct access to everything on your computer
- sourcing information about you from social media platforms
- direct requests for scans of your driver’s license or passport, often in the course of a dating and romance scam.

“No one is really selling an iPhone for \$1, or rewarding the completion of a survey with expensive electronic goods or large gift vouchers. They’re scams to get your valuable personal information,” Ms Rickard said.

“The identity thieves can make victims’ lives a nightmare. They’ll change the victims’ phone carrier so they lose service and set up mail redirections so they’re in the dark about what’s going on.”

Scammers can empty victims’ bank accounts, take out tens of thousands of dollars in bank loans under victims’ names, and purchase expensive furniture or electronics under ‘no-repayments for 12 months’ schemes.

Lost personal information also leaves victims more susceptible to future scams. Scammers will use the victim’s personal information to seem more convincing in cold calls.

“The trick is to be alert to the signs. If your mobile phone suddenly loses coverage, you haven’t received expected electronic or physical mail, or you receive unexpected notifications from a financial institution, call your bank.”

If you have been the victim of identity theft, contact [IDCARE](#) on 1300 432 273. IDCARE can guide you through the steps to reclaim your identity.