Identity theft

Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits.

Common methods of identity theft

> Phishing - the scammer tricks you into handing over your personal information.

> Hacking - the scammer gains access to your information by exploiting security weaknesses on your computer, mobile device or network.

> Remote access scams - the scammer tricks you into giving access to your computer and paying for a service you don't need.

> Malware & ransomware - Malware tricks you into installing software that allows scammers to access your files and track what you are doing, while ransomware demands payment to ‘unlock’ your computer or files.

> Fake online profiles - the scammer sets up a fake profile on a social media or dating site and sends you a ‘friend’ request.

> Document theft - the scammer gains access to your private information through unlocked mailboxes or discarded personal documents such as utility bills, insurance renewals or health care records.

Warning signs

> You receive an email, text or a phone call out of the blue asking you to ‘validate’ or ‘confirm’ your personal details by clicking on a link or opening an attachment. The message contains grammatical errors and is poorly written.

There are unexpected pop-ups on your computer or mobile device asking if you want to allow software to run.

You receive a friend request from someone you don’t know on social media.

You are unable to log into your social media or email account, or your profile has been logged into from an unusual location.

You notice that amounts of money go missing from your bank account without any explanation.

You are refused a financial service or an application for a loan or credit card has been declined.

You receive bills, invoices or receipts addressed to you for goods or services you didn’t purchase yourself.

Protect yourself

Do **not** open suspicious texts or emails – delete them.

Verify the identity of the contact by calling the relevant organisation directly – find them through an independent source such as a phone book or online search. Do not use the contact details provided in the message sent to you.

Never send money or give credit card, online account details or copies of personal documents to anyone you don’t know or trust.

Choose passwords that would be difficult for others to guess, and update them regularly. Don't use the same password for every account, and don't share them with anyone.

Secure your networks and devices with anti-virus software and a good firewall. Avoid using public computers or WiFi hotspots to access or provide personal information.

Be very careful about how much personal information you share on social network sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

When making online payments, only pay for items using a secure payment service—look for a URL starting with ‘https’ and a closed padlock symbol, or a payment provider such as PayPal.

Put a lock on your mailbox and shred or destroy any documents containing personal information before disposing of them.

Find out how to get a free copy of your credit report from the ASIC MoneySmart website. Your credit report contains important information on your credit history and is useful for checking that no one is using your name to borrow money or run up debts.

Have you been scammed?

If you think you have provided your account details, passport, tax file number, licence, Medicare or other personal identification details to a scammer, contact your bank, financial institution, or other relevant agencies immediately.

You can also contact iDcare - a free government-funded service which will work with you to develop a specific response plan to your situation and support you through the process. Visit the iDcare website or call 1300 IDCARE (432273).

We encourage you to report scams to the ACCC via the report a scam page. This helps us to warn people about current scams, monitor trends and disrupt scams where possible. Please include details of the scam contact you received, for example, email or screenshot.

We also provide guidance on protecting yourself from scams and where to get help.

Spread the word to your friends and family to protect them.

More information

Stay Smart Online - Practical tips on how to stay safe online

ID Theft - Informative video by Strathfield Council

Identity theft statistics

December 2019

Amount lost

$232 580

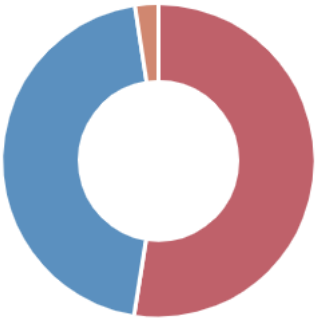
Number of reports

796

Reports with financial losses

5.8%

Gender



Male 52.5% Female 45.1% Gender X 2.4%

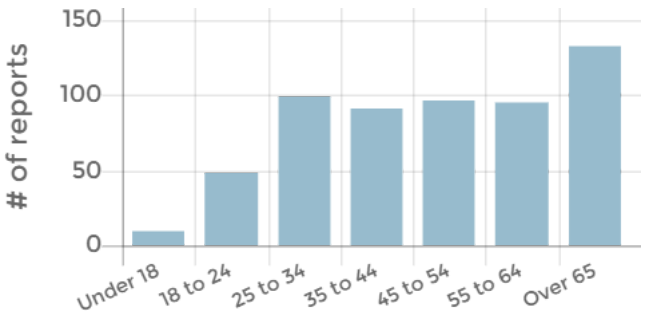
Delivery method

Phone 38.2% Email 26.5% Text message 17.2% Internet 8.2%

Social networking 3.9% Mail 2.4% In person 2.1% Mobile Applications 1.4%

Not provided 0.1%

Age



View more statistics

This data is based on reports provided to the ACCC by web form and over the phone.

The data is published on a monthly basis. Our quality assurance processes may mean the data changes from time to time.

Some upper level categories include scam reports classified under ‘Other’ or reports without a lower level classification due to insufficient detail provided. Consequently, upper level data is not an aggregation of lower level scam categories.