Q&A - Scams and identity theft

Scams Awareness Week 2020

August 2020

What is a scam?

An attempt to trick someone, usually with the intention of stealing money or personal information.

What is identity theft?

A crime in which your private information is stolen and used for further criminal activity including scams.

What types of personal information do scammers look for?

Scammers will try to find any personal information about you, including but not limited to your:

- full name
- date of birth
- place of birth
- current and previous residential addresses
- postal address
- email addresses
- phone numbers
- drivers licence number
- passport number
- Medicare number
- tax file number
- account numbers
- financial and banking information
- superannuation details
- photograph or image
- passwords.

What are some of the ways that scammers obtain your information?

- Through a variety of scams such as phishing, dating and romance scams, remote access scams and hacking to name just a few.
- Phishing is one of the most common ways scammers get your personal information. Scammers will call, email or message you, pretending to be from a real organisation or a known contact, and ask you to provide personal information.
- Scammers can find identifying information about you online such as via public records sites or on social media.
- They steal personal, business or customer records through hacking and data breaches.
- Scammers steal mail from letterboxes or rubbish bins to obtain documents containing personal information.
- They steal wallets to get access to credit or bank cards, Medicare cards and driver licences.
- Scammers also share and sell personal information stolen from victims to other criminals.

What can scammers do with your identity information?

With your personal information, scammers can:

- access and drain your bank account
- open new bank accounts in your name and take out loans or lines of credit
- take out phone plans and other contracts
- purchase expensive goods in your name
- steal your superannuation
- gain access to your government online services
- access your email to find more sensitive information
- access your social media accounts and impersonate you to scam your family and friends.

What impact can identity theft have on a victim?

Your identity is valuable and you have a lot to lose–not only money but once lost it can take years to recover your identity. Falling victim to a scam and to identity theft can also cause emotional and psychological harm.

How to protect yourself

Here are some simple steps you can take to protect yourself:

- Don't be pressured into giving away your information by someone who has contacted you.
- Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust.
- Limit what personal information you share about yourself online, including on social media.
- Check your credit report using a reputable credit reference bureau at least once every year for free, this can help you catch any unauthorised activity. Visit The Office of the Australian Information Commissioner for information.
- Avoid clicking on links in emails or messages, even if it appears to have come from a legitimate source.
- To visit a website or log into an account, type the address into the browser yourself.
- Don't provide strangers remote access to your computer, you never really know who you're dealing with.
- Use strong passwords for your accounts and internet network, and never share them with others.
- Install anti-virus software on all of your devices and keep them up-to-date.
- Lock your mailbox.
- Shred any sensitive documents you no longer need.

What can I do if I have fallen victim to a scam?

If you've lost money or given personal information to a scammer, there are steps you can take to limit the damage and protect yourself from further loss.

- If you've sent money or shared your banking or credit card details, contact your financial institution immediately.
- If the scam occurred on social media or a legitimate website, report it to the platform involved. For scams on Facebook, Messenger, WhatsApp and Instagram, see this step-by-step guide for reporting scams on Facebook services.
- If you've given your personal information to a scammer, visit IDCARE or call 1800 595 160 - Australia and New Zealand's not-for-profit national identity and cyber support service. IDCARE can work with you to develop a specific response plan to your situation and support you through the process.
- Awareness is our best defence against scams - take the time to warn your friends and family about scams.
- For more information or to report a scam visit Scamwatch.
- To keep up-to-date on scams, subscribe to Scamwatch email alerts and follow @Scamwatch_gov Twitter.
- For counselling or support services visit Scamwatch - Where to get help.

ACCC 08/20_20-18 www.accc.gov.au