# 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

# Investment scams - CRYPTOCURRENCY

Investment scams involve promises of big payouts, quick money or guaranteed returns. Always be suspicious of any investment opportunities that promise a high return with little or no risk – if it seems too good to be true, it probably is – and is highly likely to be a scam.

Australians lose more money to investment scams than any other. They can be hard to spot, so before investing always seek independent legal advice or financial advice from a financial advisor who is registered with ASIC.



## Before you invest

If you are considering investing, always remember to:

- Check if a financial advisor is registered via the ASIC website. Any business or person that offers or advises you about financial products must hold an Australian Financial Services (AFS) licence.
- Check ASIC's list of companies you should not deal with. If the company that contacted, you is on the list – do not deal with them. But even if they are not on the list it could still be a scam.
- The MoneySmart website also contains information about how to avoid investment scams.
- Search for the company online plus "review", "complaint" or "scam".

## Cryptocurrency scams

Cryptocurrencies are digital currencies. Bitcoin is the most well-known form of digital currency. In Australia, cryptocurrency is not treated as 'money' or a 'financial product' and you have less protection if you invest and it turns out be a scam or you lose a lot of money.

It is very difficult to identify legitimate cryptocurrency investments from scams. Scammers take advantage of the hype and the less regulated environment to 'invest' in Bitcoin or another cryptocurrency on your behalf.

**Before you invest** you should ask yourself if you are willing to lose some or all of the money you have invested and know that if you go ahead you are investing with little or no protections behind you.

Cryptocurrency investment scammers are convincing. They may advertise or post on social media offering great returns from cryptocurrency trading. If you click on the advertisement or post, the scammer will contact you or you will be directed to a fake website. The scammer will offer to make an investment on your behalf or provide details of an app or website through which you can invest.

Cryptocurrency scammers also commonly use platforms such as Discord and Telegram to contact people.

The scammers will encourage you to buy cryptocurrency through an exchange or request you send money to a company for them to do so on your behalf. They will then claim to either trade on your behalf, or coach you through making trades yourself. You will be able to see the profits you have made on a webpage, app or custom MetaTrader platform.

The data you can see will be fake and will show you profiting (or losing as a way to get you to invest more money). Eventually you will be unable to withdraw any money.

The scammers will make excuses for delays in withdrawals, you are banned from the platform or the trading platform is closed. When you try and find out what has happened, the scammers cannot be contacted, and your money is gone.

## Unsolicited contacts about investing

A scammer claiming to be a stockbroker or portfolio manager calls, emails or contacts you on social media and offers financial or investments advice. They may even claim to be from an investment firm or company you have heard of, as scammers sometimes impersonate these businesses to seem legitimate.

The scammer will claim what they are offering is low-risk and will provide you with quick and high returns or encourage you to invest in overseas companies.

The scammer's offer will sound legitimate, and they may have professional looking websites and resources to back up their claims. They will be persistent and may continue to contact you until you agree to invest.

The scammer may claim that they do not need an Australian Financial Services licence, or that that they are approved by a real government regulator or affiliated with a genuine company.

The investments offered in these types of cold calls are usually share, mortgage, or real estate high-return schemes, options trading or foreign currency trading. The scammer is usually operating from overseas and will not have an Australian Financial Services licence.

**Source: Australian Competition and Consumer Commission (ACCC)**

https://www.scamwatch.gov.au/types-of-scams/investments/investment-scams#protect-yourself

# 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. Scammers can also obtain your information when they hack into business or government accounts.
- 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.
- Data breaches - the scammer obtains your data through accidental data breaches of business or government accounts. You may not even be aware that some of your information has made its way to scammers.

## What scammers do with your personal 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.

## Warning signs

Before stealing your identity scammers will target your personal information. Watch out for the following signs.

- You receive an email, text or a phone call out of the blue for personal information.
- You receive an email or text asking you to 'validate' or 'confirm' your personal details by clicking on a link or opening an attachment. The message may be poorly written or contain grammatical errors.
- 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.
- Your mailbox has been broken into.

### Warning signs that your identity has been compromised

- 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 your credit card has been declined.

- You receive bills, invoices or receipts addressed to you for goods or services you didn't purchase yourself.
- You are contacted by businesses or individuals who believe they have been dealing with you even though you have had no contact with them.

## 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.
- Never provide strangers remote access to your computer – you never really know who you're dealing with.
- Choose passwords that would be difficult for others to guess. 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 Wi-Fi 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.
- 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 or Office of the Australian Information Commissioner websites. 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 1800 595 160 (if in Australia) or 0800 121 068 (if in New Zealand), or use their free Cyber First Aid Kit.

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.

Source: https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/identity-theft

# Payment demanded by gift card? It's a scam

**26 Mar 2019**

## Body

Gift cards are increasingly the payment method of choice for scammers. Scamwatch reports show more than $5 million was lost in 2018, a 38 per cent increase compared with 2017.

iTunes cards accounted for $3.1 million in losses — a 156 per cent increase from the $1.23 million reported in 2017. However Scamwatch has also seen an increase in reports involving other gift cards such as Google Play, Amazon, and Steam cards, and Australia Post Load & Go prepaid debit cards.

Losses to scams where non-iTunes gift cards were used as payment increased by 530 per cent in 2018 to around $1 million.

"Scammers like to get gift cards as payment as it's easy for them to quickly sell them on secondary markets and pocket the cash," ACCC Deputy Chair Delia Rickard said.

"It's concerning that the scammers are now demanding payment in other forms of gift cards. This is likely in response to scam warnings about using iTunes cards for paying scammers that are in stores like supermarkets and on the cards themselves."

"It's clear the scammers are diversifying their payments to try get around these warnings, so it's vital people are aware that no legitimate company or government agency will ever ask you to make a payment with any sort of gift card," Ms Rickard said.

There are several common types of scams involving gift cards:

**ATO impersonation scams**

- The scammer pretends to be from the Australian Taxation Office and claims there is a warrant for their victim's arrest. The scammer asks the victim to pay an immediate 'fine' using gift cards or bitcoin and claims police will come and arrest them if not.

**Catch-a-hacker scam**

- The scammer calls and pretends to be from a law-enforcement agency or internet provider and convinces the victim they are trying to trace the location of a hacker who has compromised the victim's computer. They claim they can do this by sending money from the victim's bank account or via gift card serial numbers.

Victims are also tricked into giving up personal details with the promise of gift cards. Scammers entice victims to participate in surveys by promising gift cards as a prize, however the surveys extract personal information such as your name, date of birth, address details and even financial details like your credit card or bank numbers.

"If anyone asks for payment using a gift card, it is a scam, simple as that," Ms Rickard said.

"If you paid a scammer with a gift card, report it as soon as possible. Call the company that issued the gift card and tell them the gift card was used in a scam. It's very difficult to get your money back but the sooner you report it, the better your chances."

Businesses that sell iTunes, Google Wallet and similar gift cards are encouraged to inform their staff about these scams so that they can help warn customers.

"If staff are informed, they can identify the warning signs of a scam when they notice a customer spending large amounts of money on gift cards," Ms Rickard said.

Further information is available online about where to get help. People can also follow @scamwatch_gov on Twitter and subscribe to Scamwatch radar alerts.

Source: https://www.scamwatch.gov.au/news-alerts/payment-demanded-by-gift-card-its-a-scam

## Don't fall for a scammer's puppy dog eyes

Puppy scammers play on people's emotions who have their heart set on a particular breed. Once they see that cute puppy picture in an ad, they drop their guard and tend to miss the warning signs that they are dealing with a scammer.

Scammers will advertise puppies they know are sought after or popular, particularly pedigree breeds. The majority of people have been contacted by scammers via email or online through classified sites and even social media.

A key sign you may be dealing with a puppy scammer is in the stories they spin. For example, scammers will often claim that they have moved interstate or overseas and that you will need to pay for transport or medical costs before the puppy can be delivered.

Another common lie involves the scammer claiming that the puppy is overseas, or even interstate and it can't be delivered unless a payment is made due to customs or quarantine issues.

If you hear these tales from a 'seller', stop all communication with them. The puppy, sadly, isn't real and if you make those payments, you'll lose your money.

**Below are some important tips you can follow to protect yourself from puppy scammers.**

- The most important tip is that old saying: 'If it seems too good to be true, it probably is.' Scammers will place ads selling pedigree pups at cheap prices. Don't fall for it for the scam.
- Don't believe the ad is legitimate just because you see it on reputable websites, social media or even your favourite newspapers.
- It's worth doing an internet search using the exact wording in the ad. Scammers get lazy and use the same wording over and over again.
- If you are in doubt, seek advice from someone in the industry such as a reputable breeders association, vet or local pet shop.

*Example pictures used in puppy scams:*

*Information obtained from Scamwatch*

*https://www.scamwatch.gov.au/news-alerts/dont-fall-for-a-scammers-puppy-dog-eyes*

# Dating and romance scams - don't let them break your heart or wallet

Dating and romance scams are very destructive – both financially and emotionally. In 2013, more money was lost to dating and romance scams than any other type of scam, with over $25 million reported lost in Australia - $7.4 Million from NSW alone.

Unfortunately, the scammers have a high rate of success, with 43 per cent of people who reported an approach by an 'admirer' losing money – on average over $21,000! These scams also cause significant emotional harm, with many victims reporting a break down in relationships with friends and family.

With the proliferation of online dating websites, forums and social media channels, these scams are moving increasingly into the online space. Online communication channels allow scammers to operate anonymously from anywhere in the world.

Source: Targeting scams: Report of the *ACCC on scams activity 2013 - Australian Competition and Consumer Commission (ACCC)*

## How these scams work

Scammers exploit their victim's emotions in order to take their money. They can be very elaborate hoaxes, sometimes taking years to develop and run by experienced criminal syndicates.

The scammer develops a strong connection with the victim before asking for money to help cover costs associated with a supposed illness, injury, family crisis, travel costs or to pursue a business or investment opportunity.

Scammers often approach their victims on legitimate dating websites before attempting to move the 'relationship' away from the safeguards that these sites put in place; communicating through other methods such as email, where they can more easily manipulate victims.

Scammers also target victims through social networking sites, where they 'like' them and then express shared interests based on personal information taken from the victim's profile.

## How to stop this happening to you

**Keep your personal details personal:** Never share personal information or photos with someone you don't know and trust – especially photos or webcam calls of a private nature. There have been reports of scammers using this material to blackmail victims.

**Watch out:** If an online admirer asks to communicate with you outside the dating website, such as through a private email address or over the phone, watch out – they could be trying to avoid detection. If you are considering meeting in person, choose a public place and let family or friends know where you are at all times.

**Search:** Run a Google Image search to check the authenticity of any photos provided. Scammers often use fake photos they've found online.

**Think twice:** Never send money to someone you've met online, especially via money order, wire transfer or international funds transfer – it's rare to recover money sent this way.

**Report:** If you think you have provided your account details to a scammer, contact your bank or financial institution immediately.

## Report Scams

If the scam originates in NSW, you can report this to the NSW Police Force by visiting your local police station or calling the Police Assistance Line on 131 444.

You can report scams to the ACCC via the 'report a scam' page on SCAMwatch. If you met the scammer through a dating service or social media, you should also inform the dating service/social channel of your experience so that they can try and stop the scammer hurting others.

## Where to find out more:

**Scamwatch** - www.scamwatch.gov.au

**NSW Fair Trading** - www.fairtrading.nsw.gov.au

**Australian Competition and Consumer Commission** - Targeting scams: Report of the ACCC on scams activity 2013 - Australian Competition and Consumer Commission (ACCC) - http://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity

Source: https://www.police.nsw.gov.au/crime/frauds_and_scams

# Scammers pretend to be the Australian Federal Police to target vulnerable people

**15 Sep 2021**

Police have received reports of scams involving fake Australian Federal Police (AFP) representatives targeting vulnerable members of the community.

Some scammers are falsely identifying themselves as a Federal Agent and telling victims they have identified suspicious activity linked to their bank accounts. They then request personal details, including a Medicare number, address, and bank details. The fake representatives ask their victim to deposit money into an AFP account.

Scammers are also targeting people using email and social media with fake arrest warrants. The offenders then call their victims and demand payments ordering them to deposit money into a nominated bank account, transfer crypto currency, or purchase online vouchers.

Some scammers ask their victim to meet in public to hand over money, or ask them to withdraw funds from their account and deposit into an AFP account.

A number of people have been manipulated by these offenders. In some cases, people have deposited thousands of dollars into a scam bank account. In other cases, people have withdrawn money from their account but fortunately, have spoken to family or friends and realised they are being scammed before handing over any funds.

Phone calls from scammers may appear to come from a legitimate AFP number. In some reports, the scammers have managed to mimic an AFP number to disguise their identity. Police suspect these calls are actually coming from overseas.

## What you need to know

- If you are contacted by someone you suspect is a scammer, end the call immediately. Do not call them back on the number they called you on.
- The AFP will never ask you to pay a fine with cash, crypto currency such as Bitcoin, gift cards such as iTunes or Google Play, and will never call you to ask to you transfer funds into a bank account.
- The AFP will never call, email or contact you via social media to threaten to arrest you, demand you withdraw money or ask you to confirm personal details over the phone.
- The AFP (and the Australian Government) will never seek payment for fines or other matters over the phone.
- If you are in any doubt, you should look up the number of the AFP switchboard in your capital city. Call and speak with a genuine AFP employee to be sure such a call demanding payment was not real.

Information obtained from Scamwatch. Link below

https://www.scamwatch.gov.au/news-alerts/scammers-pretend-to-be-the-australian-federal-police-to-target-vulnerable-people

# Websites to visit

**Flubot Scams** – Visit Scamwatch website below where there is information regarding steps on removal of the software.

https://www.scamwatch.gov.au/news-alerts/missed-delivery-call-or-voicemail-flubot-scams

**Investment Scams** – Visit Scamwatch website below for types of investment scams.

https://www.scamwatch.gov.au/types-of-scams/investments/investment-scams

If you are considering investing, always check if a financial advisor is registered via the ASIC website. Any **business or person** that offers or advises about financial products must hold an Australian Financial Services (AFS) licence.

https://asic.gov.au/for-finance-professionals/afs-licensees/financial-advisers-register/

Also check ASIC's list of companies you should not deal with.

https://moneysmart.gov.au/companies-you-should-not-deal-with

| TRIPLE ZERO (000) | POLICE ASSISTANCE LINE (131 444) | CRIME STOPPERS (1800 333 000) |
|---|---|---|
| Emergency only | For non emergencies | Report crime anonymously |

NSW Police Force
Northern Beaches PAC