Hervey Bay Neighbourhood Centre
The Heart Of Our Community

Scams and Financial Abuse

Understanding the hazards and how to protect yourself

Wide Bay Burnett Community Legal Service

Hervey Bay Neighbourhood Centre
The Heart Of Our Community

Acknowledgment to Country

We acknowledge the Butchulla people, the Traditional Custodians of the land on which we live and work, and recognise their continuing connection to land, water and community. We pay respect to Elders past, present and emerging. We extend that respect to Aboriginal and Torres Strait Islanders today.

Disclaimer

The material contained throughout this presentation is provided for general information and educative purposes. The content does not constitute legal advice or recommendations and should not be relied upon as such. Appropriate legal advice regarding your personal and specific circumstances ought to be obtained.

This document is current as at 22 May 2023. Laws may have changed in the meantime. We cannot warrant that the information contained herein will remain accurate over time. Please seek advice in relation to your specific circumstances.

Overview

1. What is identity theft?
2. What is a scam?
3. What is financial abuse?
4. What can I do to avoid becoming a victim?
5. What can I do if I am a victim?

Identity theft

- Your identity is valuable to criminals
- If a criminal can successfully convince a supplier of goods, services or financia products that they are you, they can rack up debts in your name
- To do this they need to find out enough about you to fool someone else. If they can find out your full name, date of birth and drivers licence number, that can be sufficient to convince many providers of goods, services or credit that they are dealing with a trusted person who pays their bills: you.
- Example: You have a copy of an old form which includes your drivers licence number, your date of birth, and your signature. You no longer need it, and throw it in the bin. On bin night, a criminal rifles through your bin. He retrieves that piece of paper. He also retrieves an old phone bill, and an old bank statement.

Identity Theft – cont'd

- The criminal has hit the jackpot. In clearing out your filing cabinet, you have unknowingly handed to him everything he needs to impersonate you.
- He calls Optus and orders the best iPhone Apple makes, at $2,000 each. He gives Optus your name and your billing address. He gives them your drivers licence number, but a different delivery address. Optus processes the application and does a credit check – on you. That check passes. The criminal receives a new iPhone. You receive a $2,000 account from Optus and this may be the first sign you get that identity theft has occurred.
- If you are lucky, this will be the end of it. If you are unlucky, the criminal will do this repeatedly and can rack up alarming sums of money, or worse still, sell your details on the internet to other criminals.
- It can be very difficult to convince a provider of goods, services or credit that it was not your act. They want to be paid. They will often harass the victim for lengthy periods of time before accepting that they did not enter into the contract.

Identity Theft – cont'd

- Suppliers of credit who believe you are in default of your obligations may send adverse reports to credit rating agencies. This can severely damage your credit score and make it very difficult to obtain future credit.
- Creditors can usually eventually be made to accept that you are the victim of identity theft. There is also a mechanism for removing incorrect events from credit reports however these can be time consuming, difficult and frustrating exercises, especially if the criminal has taken out credit in your name from multiple third parties.

Identity Theft - Prevention

- So how do you protect yourself from identity theft?
  - Firstly, acknowledge that your identity records and information are precious and valuable. To you, they are just your name, birthday and the drivers licence number you've had for years, but to a criminal they are gold mines.
  - Protect that information. Do not provide it to persons who do not have a clear and valid reason to require it. Keep your documents and records secure. If you have need to dispose of documents which contain sensitive identity information, you should destroy them either by burning them (where possible) or by shredding them with a cross-cut shredder. Do the job personally if you can, do not trust that someone else will do it properly. Do not leave sensitive documents lying around in your house where they might be picked up either by a visitor, or a thief.
  - SECURE YOUR EMAIL AND THE PASSWORDS TO ALL ELECTRONIC ACCOUNTS. This is one of the most important things you can do. As the world has moved into the 21st century, much of our lives are now electronic and each of us generally has an email account. Bills come there, so does official correspondence. Over years, a substantial trove of information can accumulate.

Identity Theft - Prevention

- If someone is able to obtain access to your email account, they may hit the jackpot with multiple sources of detailed information about you all in one convenient place.
- That level of information can allow criminals to conduct more complex and more damaging fraud using your identity.
- A criminal who obtains access to your email or social media accounts will often lock you out by changing the password, to slow down any efforts to prevent what they are doing. This is a red flag.
- Some criminals have become skilled at convincing telcos to churn your mobile phone number to them. The criminal then obtains a new SIM from the telco, with your number. With this, a criminal can defeat two-factor authentication systems such as the systems protecting your internet banking.
- If you cannot log into your email, when you know you have the password right, or if your lose service on your phone, and your telco tells you that the number has been churned, these are signs that you need to take urgent action.

Identity Theft - Prevention

- Treat the passwords to your online accounts like the key to your front door. It should only open that door, and not the door at any other house!
- Use a unique, memorable password for each account. It can be very tempting to use the same password for your email, internet banking, eBay and Facebook. This is an extremely bad idea. A bad actor only has to get access to the password once, and they are now able to access your entire electronic life across multiple sites and mine it for information they can abuse. **It is especially important that you secure your BANKING and EMAIL accounts with unique passwords which are not shared and never used for any other site.**
- Not all online services protect their users' security as well as you might like. Some are vulnerable to attacks which compromise users' passwords. Say you use the same password for your email, internet banking, and little cooking website that you contribute recipes to. The bad actor will struggle to defeat the security on an email or banking website, so they hit the little cooking website instead, because it's run by a volunteer and hasn't had a security update in years. From this they obtain the email addresses and passwords for all of its users.
- The bad actor now has a handy list of email addresses, and a relatively high chance that the same password will also unlock the email account. If you use different passwords for each site, a bad actor can only compromise *one at a time*. If you have trouble remembering multiple passwords (don't we all!) you can use a password manager to keep a secure list which only you can access.

Identity Theft - Prevention

- Check your credit reference regularly. It will disclose most applications for credit. If you observe any applications you did not make, this is a red flag that identity theft may have already occurred.
- There are a number of credit rating agencies and they all have a mechanism, required by law, to provide you with a free copy on request at least once per annum. You can obtain a copy more frequently than that, but the credit agency is entitled to charge a small (not excessive) fee.
- Some credit agencies, such as Equifax, offer a “credit alert” service which will proactively contact you if a credit inquiry is made on your file. This can provide you with early warning that someone may be applying for credit in your name. A fee may be payable for such services.
- Bear in mind that credit agencies maintain separate files on individuals, and they may not be identical. Inquiries with one may not automatically appear in the records of another. You may need to check multiple providers to obtain a full picture of your credit record.

Identity Theft - Recovery

It can be a slow and painful process to recover from identity theft. It is far preferable to prevent it in the first place.

- **Unless you are aware of exactly how your identity was compromised, and to what extent, you may have to assume that all forms of identification are compromised.**
- **You may have to deal with the motor registry, to change your licence number, with the banks to change your passwords, you may have to go through a recovery process with your email supplier to convince them that you are who you say you are, and have your password reset. You may have to deal with multiple creditors who believe that they have supplied goods or services to you, and who may be less than willing to accept that they, too, were scammed and that you should not have to pay them.**
- **It can take a year or more in some cases to finally free yourself from what has occurred.**

Identity Theft - Recovery

- If you believe you have been a victim of identity theft you should immediately contact your bank(s) and advise them, have them secure your account, check that there are no unusual transactions, and reissue your internet banking login credentials.
- If you have access to your emails, change the password immediately. If the criminal has changed it already, you may need to go through a password recovery process with the email provider. This may require you to know the answers to certain key challenge questions. If you set your account up a long time ago, check that you still know the answers to the challenge questions. Those should be answers which no other person could easily guess.
- Change the passwords on any other site which may have been compromised.
- Call Police and make a report.

Identity Theft - Recovery

- **IDCARE** is 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.

- **WWW.IDCARE.ORG 1800 595 160**

Identity Theft - Recovery

- If you have been a victim of Commonwealth Identity Theft, the Department of Home Affairs can issue you with a Commonwealth Victims Certificate, which can make it easier to prove your have been a victim of identity theft.
- The following types of identity theft can enable a Certificate:

- your birth certificate was used by someone else to falsely claim a payment from Centrelink in your name
- a person pretended to be you by using your identification details to have your Medicare rebates redirected to their bank account
- a person used your credit card without your permission to purchase and import illegal substances
- a person established a false business in your name to fraudulently claim GST
- a person used your passport or citizenship details to pass themselves off as you and travel overseas

Scams

- Scams are carried out by criminals, and frequently by a total stranger.
- Identity theft is a specific form of scam, but the number and inventiveness of scammers has been on the rise for quite some time, facilitated by the transition to electronic communication. Cheap access to telecommunications has allowed whole industries to thrive in some (mostly developing) countries, just to scam people in more wealthy countries.
- Scammers set out to fool their victim into voluntarily handing over money or assets by pretending to be someone they are not, such as an official agency, or a business that you interact with. To succeed, they must first establish their own legitimacy in your mind, and maintain that for long enough to complete the scam.
- Scammers try to take advantage of naivete, but also of greed and of fear. An offer that sounds too good to be true is an appeal to greed. A phonecall that tells you something awful will happen if you don't pay is an appeal to fear.

SCAMS - Examples

- The “lonely hearts” scam is a common trap. In this scam, you will be contacted out of the blue by an attractive, and often much younger, member of the opposite sex who lives in another country, usually a developing country.
- Lonely hearts scammers send out hundreds of these emails, often to lists of email addresses they have bought or obtained online. Most people ignore them, but a few, often lonely mature people, fall for it. A desire for friendship can blind their usual judgement.
- A long distance relationship then appears to develop over time, usually with exchanges of many emails or phone calls of a deep and personal nature which lead the victim to believe that a true connection is being established.
- Soon after, some disaster such as a medical emergency will befall your new friend. They will tell you that they are in great distress and that you are their only hope. A request for money soon follows.
- Unfortunately once a lonely hearts scammer knows that they have your confidence, they will usually escalate their requests for money. It is not unusual for a victim to make multiple payments over time which can add up to really significant sums of money.
- Suffice to say that these “relationships” rarely have a happy ending.

SCAMS - Examples

- You receive an email from a solicitor overseas. She says that she is acting in an estate for one of your long lost relatives. It is a substantial estate, and there are no other beneficiaries. It took a long time to find you, and they would like to give you a lot of money. Isn't that lovely? Had no idea I had an Aunty Giselle in Germany, but hey, free money! But wait. Before they can send you all this lovely money, for various complicated reasons they first need you to pay some money to them. The reasons will sound feasible and believable. If you send the money, it is almost certainly gone for good. But wait. The scammer now knows you're a live one. He thinks maybe he can go again. A new complicated story appears, your money is really close now, but you just have to pay a bit more to get it. So you do – and that money is likely gone for good too.
- You receive a recorded phonecall from the Australian Passport office. A stern voice advises you that you are in a great deal of trouble for some imagined offence. There will be criminal charges and you may be jailed – but you can avoid all that unpleasantness if you immediately pay a substantial fine - in Apple gift cards.

SCAMS - Examples

- You receive a telephone call from Microsoft, or Telstra. You are told that their systems have discovered a problem of some kind with your computer, and it is putting you at risk, or slowing down your machine. They offer to help you fix it. In order to do so, they ask you to install a small piece of software that lets them see your screen. They then have you do various things to address the problem, and at some point they might have you log in to your email, or your internet banking. Their software is capturing your keystrokes. Soon the problem is "resolved", the scammer is off the phone and you can no longer log in to your email or bank account. If you used the same password, then you can no longer log in to either!
- You are now at great risk.
- There are far too many scams, and more being invented all the time, to list them all here, but we'd like to point out one more recent very serious one. A person had contracted to buy a house in WA, and was due to deposit the purchase moneys, of around $732,000, into her settlement agent's trust account. Scammers managed, perhaps by breaching an email account, to intercept her settlement agent's instructions for payment, and sent the buyer a fake email substituting their own bank details. The purchaser paid the money into that account. This is known as a "payment-redirection" or "man-in-the-middle" attack. This year so far in the same State, the combined loss from this form of attack is over $1M. In 2021, 37 victims lost over $1M combined. Only two victims recovered around $287,000 of their losses.
- But what can you do to not fall victim?

SCAMS - Prevention

- First and foremost – BE AWARE. This can happen to ANYONE. It is being done at such a scale that there is no safety in numbers, very few of us can completely avoid scam attempts. We can avoid actually being scammed.
- Secondly, BE LESS TRUSTING. The world is not the place it was. If you receive a call or an email you were not expecting, work from the presumption that it is a scam until proven otherwise.
- If something sounds too good to be true, it is.
- READ your emails carefully and look for errors or anything that's not quite right. Spelling and grammatical errors are common in scam emails sent by people for whom English is not their first language, and it may be sent from an email address such as Hotmail or Gmail which a professional business generally wouldn't use. It is VERY important that you are confident that an email is genuine before you click on any link. Scam emails often contain links to dangerous websites or for installation of malicious software. For instance, you may be sent an email which looks like it has come from your bank, asking you to log in for some reason. If you click the link, you will be taken to a page which looks exactly like your internet banking site. If you enter your credentials, the scammers can capture them and then login to your real account. If in doubt – VALIDATE.

SCAMS - Prevention

- INDEPENDENTLY VALIDATE what is being said to you. If an employee of a Government body, a bank, your internet provider, or anyone else wants to speak with you, they will provide you with their name and title and should be able to tell you how they can be reached from the main phone line of the agency or business allegedly calling you. If you receive a call, for instance, from the Passport Office saying alarming things, you should remain calm, ask the caller for their name, title and phone extension, and tell them you will call them back shortly. You should the obtain the phone number for the Passports Office from an independent source such as the phone book, or the official government website and call only that official number. The caller may attempt to provide you with a "direct number" for callback, or tell you it will be too hard to reach them through the company's phone system – this defeats the purpose of verification, don't fall for it. You should call a known valid number from a trustworthy source and then ask to speak to the person who called you, or otherwise seek to verify what you were told.
- No professional organisation operating in a businesslike manner should fail this test. If the test fails, you should assume it is a scam and proceed no further. You should also report the scam attempt to the organisation.

SCAMS - Prevention

- The Commonwealth Government operates a website which tracks common scams and advises what to look out for, and how to keep yourself safe.

WWW.SCAMWATCH.GOV.AU

SCAMS – How do I recover?

- If you have been the victim of a scam, you should act quickly - as soon as you realise, DO NOT DELAY. You may well feel ashamed or foolish. You are neither, you are a victim and there may be help available if you act quickly. The more time you give the scammer, the more likely it is that they will get away with it.
- If you have made transactions from your online banking account, call the bank as a matter of great urgency. If you act quickly enough you may be able to get certain transactions blocked or reversed.
- If you have voluntarily given money or valuables to a scammer, even if under false pretences, it may not be possible to recover them and it may not be possible to seek to have anyone else, such as your bank, repay you.
- You may have suffered identity theft during the course of the scam, in which case you will need to look at all the same recovery actions discussed for identity theft.
- If your passwords were compromised you will need to take the same steps discussed in relation to identity theft – recover the accounts and set new passwords.
- You may have other recovery options. Seek legal advice as soon as possible.

Financial Abuse

- Financial abuse is when someone prevents you accessing your money, controls or manipulates your financial decisions, or takes and uses your money without your consent.
- Financial abuse is often carried out by someone you know, and often by someone you thought you could or should have been able to trust - a partner, a family member or a carer.
- Financial abuse is a common form of domestic violence.
- Motives for financial abuse vary. In some cases it is done to exert coercive control and undue influence, as in domestic violence.
- In other cases the person steals from you because they think they can get away with it. This is especially dangerous for senior people with diminished capacity as they are highly vulnerable.

Senior Financial Abuse

- **Examples of senior financial abuse:**
- Uses the older person's money without their consent or knowledge
- Signs legal documents on behalf of an older person
- Threatens or punishes an older person if they don't give the perpetrator money
- Makes the older person think that they can't manage their own money
- Selling or disposing the older person's property without permission
- Shopping for an older person and not returning any change
- Not repaying loans
- Not contributing to household expenses
- Misusing financial powers under an Enduring Power of Attorney
- Taking advantage of the sharing of resources within families

Financial Abuse - Prevention

- Be careful who you trust. Unfortunately sometimes it can be difficult to know who to trust, and sadly in some cases people who seem trustworthy can turn out not to be. Consider carefully before you hand your keycard, it's PIN, your wallet (with your ID documents) or similar high-risk items to anyone else. The terms and conditions of your contract with the bank will usually prohibit you from allowing another person to use your card, for good reason. If you do it anyway, then at the very least make sure the card is out of your sight only for as long as required to do what you have authorised – and check your account afterwards to confirm that was all that was done.
- Secure your ID. If an abuser can get control of enough of your ID information they can carry out an identity theft. This has resulted for instance in people having real estate sold without their knowledge or consent, because the abuser was able to gather enough material – including the title deeds - to convince a bank and solicitors that they were the victim. Consider investing in a small lockable box or safe to store such documents. Important documents can often be held in safe custody by a bank or a law firm if you have concerns about the security of your home environment.

Financial Abuse - Prevention

- Money is a temptation for many people. Some may assume you no longer need it, or convince themselves you would not mind. Regrettably some children believe it is okay to help themselves to an “early inheritance”, perhaps because they think it will come to them eventually anyway.
- If you are of sound mind and body, give careful thought to the future. What arrangements might you need in place to keep you financially safe if you become unable to manage your own affairs? This is quite specific to each individual. You should strongly consider obtaining legal advice whilst you are still well and able to make good decisions.
- It is not unusual for a person, especially an older one, to grant a trusted child or children, or other trusted parties, Power of Attorney to manage their financial affairs if they lose capacity.

Financial Abuse - Prevention

- A power of attorney often gives broad or unfettered right to the appointee to operate your financial affairs. HOWEVER, the law requires that the Attorney act in your best interest at all times while doing so, and unless expressly stated the Attorney cannot apply any of your money to their own benefit.
- This unfortunately does not stop some attorneys from doing just that.
- You can limit the operation of powers of attorney, to provide a little more safety. For instance, you can stipulate that it does not come into effect unless and until a certain event happens, or it can stipulate limits to the Attorney's powers in general, such as which assets or affairs they can deal with, and which they cannot.
- It can be very difficult to strike a balance between placing prudent controls on the Attorney, and tying their hands. Once you lose capacity, you will no longer be able to change the terms of the appointment. A Tribunal application would be required.

Financial Abuse - Prevention

- The best protection from elder financial abuse are eyeballs. Abusers generally conduct their crimes secretly and without anyone's knowledge. They can do a great deal of damage before their conduct is detected. If you can arrange to have more than one person keeping an eye on your wellbeing and your finances, that will limit the risk to you.
- If you do not know who to trust, or have nobody you can trust, you can consider appointing the Public Trustee to manage your finances in the event that you lose capacity to manage your own affairs.

Financial Abuse - Recovery

- **So what can you do if you believe you have been financially abused, or if you believe you are witnessing financial abuse of a senior?**
- Contact the vulnerable persons unit of the Queensland Police Service, if the abuse is current or ongoing, this may be a route to halting it early.
- Seek legal advice, including from the **Seniors Legal Advice and Support Service (SLASS)** at HBNC – you can reach us on **4124 6863**
- **Community Legal Centres** across the State are also able to provide advice and guidance.

Financial Abuse - Recovery

- **If you believe you have witnessed financial abuse:**
- Don’t ignore it
- Ensure that your actions are respectful of the older person’s rights and choices
- Contact emergency services if there is an immediate risk of harm
- Gather information by asking questions sensitively. Some questions you may be able to ask include:
  - How are things going at home?
  - How do you feel about the amount of help you get at home?
  - How do you feel your (husband/daughter/carer etc) is managing?
  - How are you managing financially?

Financial Abuse - Recovery

- **If you believe you have witnessed financial abuse – cont'd**

- Record the details – eg. what you saw and/or heard and when. This record should be in writing and must be kept confidential
- Do not take matters into your own hands
- Seek legal advice including from police and/or from our SLASS unit.

Important takeaways

- The world has become a more complex and risky place. Those complexities and risks have increased as a result of changes to technology.
- Complacency can cause significant loss.
- Treat your electronic passwords like the key to a valuable safe. Only one key should open each lock, and you should be the only one who has it. It should not open any other locks!
- VERIFY official communications from companies or organisations by using their official contact channels to double check what you have been told.
- If it looks too good to be true, it is!
- It's sad to say it, but be less trusting. Scammers and criminals take advantage of our good natures. We can prefer to believe that people are good until proven otherwise, and that's a lovely philosophy for life but it is naïve approach to risk.

Important takeaways

- Consider enlisting the help of trusted friends or family to do a “digital audit” with you, to go through all of the potential attack methods and make sure that your accounts are as secure as they can be.
- Act as soon as you suspect there may be a problem, the quicker you act the better the chance of limiting the damage. If your bank account may be involved, call the bank first!
- Seek legal advice and referral to agencies who can assist you. We have a Seniors Legal Advice and Support Service with caseworkers who can assist if the victim is over 60 years of age (55 for ATSI clients), and the Wide Bay Burnett Community Legal Service which is open to the entire community.
- There is no place for shame or guilt. Victims are not fools, they are victims. Reach out and get the assistance you need.

Questions

If you would like specific advice you may contact our Reception for an appointment:

- Wide Bay Burnett Community Legal Service (07) 4194 2663
- Seniors Legal Advice and Support Service (07) 4124 6863