Scams: *Information Sheet*

Scams are fraudulent schemes/transactions designed to deceive you for financial gain or other benefits. They can take many forms and are perpetrated through various mediums, including phone calls, emails, text messages, social media and in-person interactions. Understanding common scams and how to recognise them is essential for protecting yourself and your assets.

Identifying a Scam

The main types of scams you may encounter are:

1. **Phishing Scams:** Phishing scams involve fraudulent attempts to obtain sensitive information, such as passwords, credit card numbers, or identification information, by posing as a trustworthy organisation. This often occurs via email, where scammers impersonate banks, government agencies or reputable companies to trick victims into providing their personal information.
2. **Investment Scams:** Investment scams promise high returns with little or no risk. These schemes often target individuals looking to make quick profits and may involve fake investment opportunities, Ponzi schemes, or fraudulent trading platforms. These types of scams often seek out those with self-managed superannuation/significant savings- which tends to focus on older Australians.
3. **Tech Support Scams:** Tech support scams typically involve cold calls or pop-up messages claiming to be from a reputable tech company and offer a quick fix. The scammers trick victims into believing their computer has a virus or security issue, and then offer to fix it for a fee. The scammer then will usually gain access to a computer to 'fix' the issue and either steal personal information or take control of the computer to extort the end user.
4. **Romance Scams:** Romance scams occur when a scammer builds a romantic relationship with their victim, often through online dating platforms, and then requests money under false pretences. These scams can be emotionally devastating and result in significant financial losses.
5. **Lottery or Sweepstakes Scams:** Lottery or sweepstakes scams notify victims that they've won a prize but must pay fees or taxes to claim it. In reality, there is no prize and the scammers pocket the money sent by the victims. They also harvest information and are a form of phishing scam.
6. **Charity Scams:** Charity scams exploit people's generosity by soliciting donations for fake or non-existent charitable causes. Scammers may impersonate legitimate charities or create fraudulent organisations to deceive donors.
7. **Shopping/Marketplace/Payment Scams:** This can include the advertising of a vehicle/item at a very good price, that turns out to not exist or be faulty or not as described. It may require a deposit/payment to be made before seeing the item. It can be local (as in a fraudulent local

person) or internationally based. It may involve the use of fraudulent shipping/payment information and tends to involve payment platforms where transactions cannot be challenged/reversed (*Paypal, Friends and Family*, *PAYID, OSKO* etc). This usually occurs through Facebook/Gumtree where the platform is "buyer beware" and less commonly through services such as *eBa*y/*Amazon* that have greater controls.

8. **SMS / Message Scams:** These types of scams usually involve a message from a purported business/person you know requesting action via a link or payment to be made. Examples of this type of scam include SMS message purporting to be from a relative requesting money or alerting you that you need to pay a parking ticket/toll charge.

Warning Signs of Scams

Scams are constantly evolving to keep ahead of the game. However, the following are common occurrences when being scammed:

- **Unsolicited Contact:** Be cautious of out of the blue phone calls, emails, text messages or social media messages, especially if they request personal or financial information.
- **Pressure to Act Quickly:** Scammers often create a sense of urgency or fear to pressure victims into making rash decisions without thinking things through. Take the time to undertake enquiries (i.e., to call the legitimate business/family member to confirm authenticity).
- **Too Good to Be True Offers:** If an offer seems too good to be true, it likely is. Exercise scepticism towards promises of high returns with little or no risk. Your Nigerian Prince may in fact turn out to be a toad.
- **Requests for Payment or Personal Information:** Be wary of requests for payment upfront or demands for personal information, such as passwords or *Medicare*/*Centrelink* numbers.
- **Poor Grammar and Spelling:** Many scams originate from non-native English speakers and contain grammatical errors or awkward language usage. However, the introduction of AI is assisting scammers in this regard. Another common feature of email scams is that the email username when clicked on reveals an unrelated email address (i.e., a scam email from *Microsoft* may have typographical errors or an unrelated domain name such as mycrosoft@microsoft.com.ky).
- **Recent Creation:** A scammer may create a *Facebook*/online presence to add legitimacy to their scam. For example, if a business has a *Facebook* page then it is prudent to research the business independently (i.e., by searching the address on *Google Street View* and checking ABN numbers are prominent and legitimate through a free ABN search etc).

Protecting Yourself from Scams

The following are some suggestions as to how you may protect yourself from scams:

- **Stay Informed:** Educate yourself about common scams and warning signs. Knowledge is your best defence against fraud.

- **Verify Information:** Before providing personal or financial information or making a payment, verify the legitimacy of the request by contacting the company or organisation directly using trusted contact information. Do not contact the company using information provided by them - use a trusted source such as the *Yellow Pages* that is harder to fake. If the issue is a purported virus in your computer, disconnect it from power and seek advice locally.
- **Use Secure Channels:** Ensure that websites you visit are secure (look for "https://" in the URL) and use secure payment methods when making online transactions such as *Paypal*. However, be aware of the terms of what you are using - i.e., *Paypal 'Family and Friends' does* not have the protections of the traditional '*Paypal'*.
- **Trust Your Instincts:** If something feels off or too good to be true, trust your instincts and proceed with caution. Seek advice from a service such as ours or speak with a savvy friend or family member who is knowledgeable as to what to look out for.
- **Report Suspected Scams:** If you encounter a scam or believe you've been targeted, report it to the appropriate authorities, such as *Scamwatch* or your local consumer protection agency (*Consumer Building and Occupation Services* (*CBOS*) in Tasmania.

What To Do If You Suspect You Have Been Scammed?

What you should do about a scam will to a certain degree depend on the nature and type of scam you are facing. However, if you believe you have been scammed, act quickly and consider doing the following:

1. Cease all contact (although keep copies of any messages) and do not continue to pay/send any money. If you have provided personal information, change your password and notify relevant service providers (i.e., contact the Tasmanian Government for a new licence if you believe your licence information is compromised);

2. Contact your bank financial institution/superannuation fund and advise them that you believe you have been scammed and the nature of the scam. Ask the bank for advice to cease further transactions/protect your accounts moving forward. Depending on how any transaction occurred, the bank may be able to retrieve/dispute the transaction

3. Seek advice urgently from:

    a. *IDCARE*- 1800 595 160 (Monday to Friday, 8am–5pm)- Australia's national identity and cyber support service which is free to use and can assist you to develop a plan to deal with what has occurred; and/or

    b. A lawyer including *North West Community Legal Centre Inc*. Depending on what has occurred and who the scam involves, there may be options to pursue a civil case to secure / recover funds.

4. Make a report to:

    a. **The *Australian Cyber Security Centre via ReportCyber***- a national Policing initiative to make a report:
    https://www.cyber.gov.au/report-and-recover/report

    b. **The *National Anti-Scam Centre* (*formerly ScamWatch*)-** a service to report a scam generally to:
    https://www.scamwatch.gov.au/report-a-scam

    c. **Tasmania Police** - by contacting 131 444 (*Tasmania Police* non-emergency line) or attending your local Police Station.

    d. ***Consumer Building and Occupational Services* (*CBOS*):**
    https://cbos.tas.gov.au/topics/products-services/buying/report-a-scam

5. If the scam relates to your personal devices (mobile phone, iPad, computer), run an anti-virus/anti-malware program and seek professional advice from an IT expert to ensure your device does not continue to be compromised moving forward. You may also contact the *Australian Cyber Security Hotline* on 1300 292 371 (open 24/7) for expert cyber security advice and assistance.

6. If you feel comfortable, make your friends aware of the nature of the scam so that they may avoid it themselves.

7. Continue to monitor your accounts/credit score and be alert to the potential for further contact from scammers. Once scammed, a person is likely to be contacted again in future as the scammer is aware they have had some degree of success.

8. Seek mental health support if you feel you need it. It is important to look after yourself.

If you are not sure where to start, please contact *North West Community Legal Centre Inc.* and we can point you in the right direction.

Seeking Advice

Scams are becoming more prevalent and sophisticated, making it essential to remain vigilant and informed. By recognising common scam tactics, staying cautious of unsolicited requests, and taking proactive measures to protect yourself, you can reduce the risk of falling victim to scams and safeguard your financial well-being.

If you require advice relating to a scam, you may contact *North West Community Legal Centre Inc.* to make an appointment. It is always best to get advice before rather than after the fact.

Other Helpful Links / Resources

National Anti-Scam Centre (ScamWatch): https://www.scamwatch.gov.au/

MoneySmart: https://moneysmart.gov.au/online-safety

Australian Cyber Security Centre: https://www.cyber.gov.au/scams

Consumer Building and Occupational Services (CBOS- formerly Consumer Affairs Tasmania) https://cbos.tas.gov.au/topics/products-services/buying/scams

Financial Rights Legal Centre Scam Fact Sheet: https://financialrights.org.au/factsheet/scams/

Published: August 2024

North West Community Legal Centre Inc.
56 Formby Road
DEVONPORT, TAS, 7310
Ph: (03) 6424 8720
Email: office@nwclc.org.au
Website: www.nwclc.org.au

Disclaimer: *This document is provided for informational purposes only. The information contained in this document may not be appropriate to your specific circumstances and whilst all endeavours have been made to ensure its accuracy at the time of publication, it may not be accurate at the time of reading. You should seek independent legal advice with respect to your individual circumstances.*

The financial assistance provided to the NWCLC from both the State and Commonwealth Governments via the National Legal Assistance Partnership (NLAP) is gratefully acknowledged.