Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**
Consumer Protection

WA ScamNet

Spotting scams

WA ScamNet profiles the most prevalent scams targeting Western Australians and provides information on different types of scams, how to recognise scams, and what to do if you have received a scam. It also provides links to other useful websites.

WA ScamNet gathers information from consumers and businesses and profiles scams that have targeted Western Australians. Simply by sending in your suspect emails and letters, Consumer Protection can identify the most prevalent scams and provide information to law enforcement agencies here in Australian and overseas.

The hot deal

If it seems too good to be true, then it is. Scammers may use a "hot deal" to entice you such as:

- a financial windfall (investment, beneficiary, ATO rebate, lottery scams, lucky charms);
- a non-existent online bargain (rental accommodation, kitten/puppy, car/boat, concert tickets);
- online selling - online sellers can become victims if the fraudulent buyer appears to have 'accidentally' overpaid by either giving you a fake fund transfer email confirmation, or they have used stolen credit card details. In both instances, the fraudster will ask for a refund of the 'overpayment' and ask that you put it in a different bank account. Other sellers have been persuaded to wire transfer money to a fictitious freight company.
- itinerant traders/door-to-door scammers (bitumen bandits, roof repairers, art students).

The urgent threat

A scammer may use a threat to coerce you into handing over personal information and money. Remember to stay in control of the situation and verify details yourself. Threats can come in the form of:

- A threat of legal action – a caller says that you will be charged/arrested unless you pay money immediately. They then ask you to go and buy iTunes cards, gift cards or Bitcoin to pay the outstanding debt, then ask you to read out the codes on the back of the cards over the phone.
- A 'help me' email – a scammer hacks a friend's email account, and sends an email asking for urgent funds. Your guard will be down because the "friend" will usually appear to be in a desperate situation and the email is coming from your friend's account.
- Windows/Microsoft/Apple/phone provider/NBN support scam – a caller says they've detected an issue with your computer or internet connection, or you have been the victim of a computer hack and they need your help to catch the hacker. The scammer will either offer to repair your computer for a fee, or coerce you into giving them access to your computer to allow them to fix the problem.
- Ransomware – your computer's files are 'encrypted' until you pay a ransom. If you've been locked out or had files encrypted don't pay a ransom as it will only encourage the scammers to extort more money from you. Use a different device to search online for a solution or seek help from a local computer technician.
- An online romancer – who suddenly needs money either for a desperate situation (such as paying for urgent surgery), or to travel to visit you.

Phishing for your details

With just enough of your personal details scammers can shop with your cards, borrow money in your name and infiltrate (hack) your accounts by guessing passwords or answers to the security questions you chose when you set them up. Be careful with your personal information and be wary of:

- **Unsecure Wi-Fi hotspots:** Do not log into important accounts on unsecure Wi-Fi. The details you enter are unencrypted and can be seen by people looking to steal your information.
- **Keylogger software/spyware:** Keyloggers and spyware track your movements online, logging what websites you visit and what you type on your keyboard. They are then able to steal your login information for important personal accounts. Keep your antivirus software up-to-date to avoid spyware.
- **Copy-cat emails and websites:** Scammers send out emails or create websites that look like they are from a real business but are designed to mislead you into providing your personal information or downloading a file that infects your computer with a virus or spyware.

Protect what you believe

- Maintain a healthy scepticism.
- Stay in control and always verify information, advice and contact details independently.

Protect your passwords

- Use passwords that are difficult to predict and different for each account.
- Generate and store passwords in a reputable password manager with two-factor authentication.

Protect your computer (and smart devices)

- Use up-to-date firewall and antivirus software.
- Update software from the source, not from pop-up windows.
- Set up your antivirus software to perform automatic updates when connected to the internet.
- Don't do anything beyond basic web surfing on unsecure Wi-Fi hotspots.
- Don't open attachments or click links from strange emails.
- Regularly back up your data.
- Don't pay a ransom – it will only encourage the scammers to extort more money from you.

When using social media

- Use the settings to set your privacy level to high.
- Limit the information you share.
- Reject friend requests from strangers.

When dating online

- Be wary of anyone that says they are based overseas or can't meet in person.
- 'Grooming' can occur for months and sometimes includes overseas flights.
- Alarm bells should ring if someone requests money, especially if you have not met face-to-face.
- Do a google image search to see if their photo has been used in another scam.
- Let friends/family who are online dating know the above information.

When sending sensitive info online

- In the search bar, look for:
- https (the 's' at the end stands for 'secure');
- green for 'go'; and
- the locked padlock.

If you have lost money to a scammer…

- Contact your bank and use your credit card 'chargeback' rights.
- Visit www.idcare.org or call 1300 IDCARE (1300 432 273) for advice.
- Beware of secondary scams offering you assistance.

Protect your money

- Lock your post box.
- Never wire transfer money to someone you haven't met.

Check bank and credit card statements and get your free annual credit report from

Equifax: www.mycreditfile.com.au

Dun and Bradstreet: www.checkyourcredit.com.au

Experian: www.experian.com.au

Other steps to minimise contact with scammers

- Log your details on the Do Not Call Register either online by visiting www.donotcall.gov.au or by phoning 1300 792 958.

Do Not Call Register

- Place a "Do Not Knock" sticker on your door.

- Report a cybercrime to the Cyber Reporting System via www.cyber.gov.au/report
- Visit www.scamnet.wa.gov.au and sign up to WA ScamNet alerts to be informed of scams targeting Western Australia.

Disclaimer – The information contained in this fact sheet is provided as general information and a guide only. It should not be relied upon as legal advice or as an accurate statement of the relevant legislation provisions. If you are uncertain as to your legal obligations, you should obtain independent legal advice.

Consumer Protection | Department of Mines, Industry Regulation and Safety
1300 304 054

8.30 am – 5.00 pm Mon, Tue, Wed and Fri
9.00 am – 5.00 pm Thurs
Gordon Stephenson House
Level 2, 140 William Street
Western Australia 6000
M: **Locked Bag 100, East Perth WA 6892**
W: **www.scamnet.wa.gov.au**
E: **consumer@dmirs.wa.gov.au**

Regional Offices

Goldfields/Esperance	(08) 9021 9494
Great Southern	(08) 9842 8366
Kimberley	(08) 9191 8400
Mid-West	(08) 9920 9800
North-West	(08) 9185 0900
South-West	(08) 9722 2888

National Relay Service: 13 36 77

Translating and Interpreting Service (TIS): 13 14 50

This publication is available in other formats on request to assist people with special needs.

DMIRSOCT19_6131