Department of **Energy, Mines, Industry Regulation and Safety**
Consumer Protection

GOVERNMENT OF WESTERN AUSTRALIA

WA ScamNet

Spotting scams

Scams can be clever and tricky, but there are steps you can take to protect yourself:

Practise the pause:

- When you get a message by phone, SMS, or email, stop and take the time to work out if it is a real message or a scam.
- Never click on links in messages or a pop-up window to update software or personal information. Banks and trusted authorities, such as government agencies, will never send you a text message with a link to update your details.
- Never give a caller remote access to your devices.

Verify with the source:

- Check you are dealing with the actual person or organisation.
- Don't give money or ID documents to anyone you have not met in person.
- Use the number or email address you already have, for example on an account statement. Or look up the contact details on an official website.
- Don't reply to the email or call the number provided in the message as you could be speaking to the scammer.
- If you are not sure, ask a trusted family member or friend.
- Contact WA ScamNet to help you work out if it is a scam.

Protect your computer, devices and accounts:

- Keep your anti-virus and anti-spyware software up to date.
- Always update software from your device's settings.
- Turn on multi-factor authentication if you can. This makes it harder for hackers to get into your accounts because they'll need more than just your username and password.

When shopping online or on social media platforms:

- Before you give money or personal information, do some research. Learn more about the company or person you're dealing with.
- Always use safe ways to pay such as credit card. If a seller wants urgent payment be suspicious.
- Be extra cautious if they ask you to pay with electronic transfers, gift cards, or cryptocurrency.
- Check online for reviews written by customers who are not affiliated with the company.
- If it sounds too good to be true it probably is. Be suspicious of products sold at heavily reduced prices.
- Always make sure to confirm payment details with the company directly before you pay an invoice that was sent to you by email.

Take action if you have been scammed:

- If you've lost money to a scam, contact your bank or financial institution right away to prevent further fraudulent transactions on your accounts.
- If you think a scammer has your personal information or identification contact IDCARE. You can call them on 1800 595 160 or visit their website www.idcare.org.
- Report the scam to WA ScamNet. Call us on **1300 30 40 54** or visit www.scamnet.wa.gov.au
- Report your scam to the Cybercrime Police. Visit the Australian Cyber Security Centre (ACSC) www.cyber.gov.au/report. Or call the Australian Cyber Security Hotline on 1300 292 371.
- If someone else has been able to control your computer via remote access, or if you think someone has hacked your computer, you should have a skilled computer expert check it.

Department of Energy, Mines, Industry Regulation and Safety
www.demirs.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

Consumer Protection Division
Gordon Stephenson House
Level 2/140 William Street
Perth Western Australia 6000
Locked Bag 100, East Perth WA 6892
Call: 1300 30 40 54
Email: consumer@demirs.wa.gov.au
www.consumerprotection.wa.gov.au

DEMIRS AUG_249157