GOVERNMENT OF WESTERN AUSTRALIA

CONSUMER PROTECTION WESTERN AUSTRALIA

Got a question? ASK us

Phishing Scams

Attempts to gain personal information

Phishing scammers get to us through email, phone or text messages.

They want to steal passwords, account numbers, and personal details to get control of your email, bank, or other accounts.

Phishing scammers pretend to be a real business, bank or government agency, and trick you into clicking on a link or opening an attachment.

Warning signs

- You receive an email, text or phone call pretending to be from a business, bank or government agency, asking you to update or verify your details.
- The email or text message does not use your name, and has spelling errors and mistakes.
- The website address does not look right and asks for details you do not normally give.
- The scammer asks to confirm your personal details or fill out a customer survey and may offer a prize/gift card.

Protect yourself

- Look out for random text messages or calls that want you to call a number or click on a link.
- If you need to contact a business, bank or government agency, find the right phone number yourself by searching for it online – do not use details given by SMS or email.
- Guard your personal and banking information and do not give account details over the phone.
- Only download things to your phone from secure locations like the App Store or Google Play.

Help if you have been phished

- Immediately contact your bank or financial institution to try and stop payments coming out.
- If you gave out personal information (or have concerns about identity theft) contact IDCARE at **www.idcare.org** or call 1800 595 160.
- Lodge a cybercrime report at Australian Cyber Security Centre **www.cyber.gov.au/acsc/report** and WA ScamNet **www.scamnet.wa.gov.au** or call **1300 30 40 54**.

SCAN ME

WA ScamNet

DMIRSJAN238022