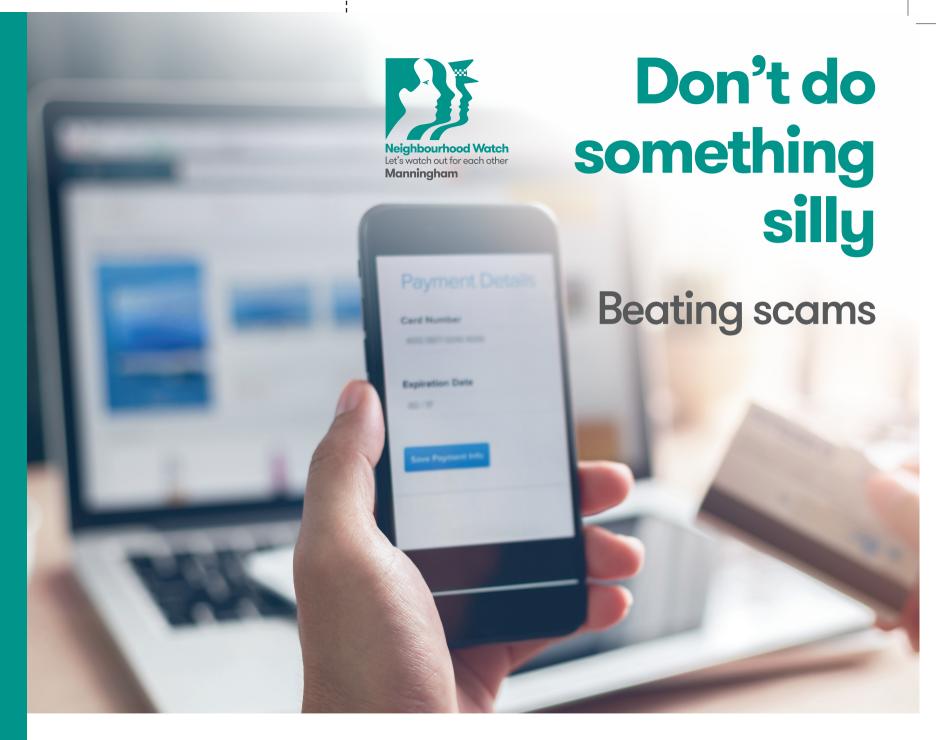


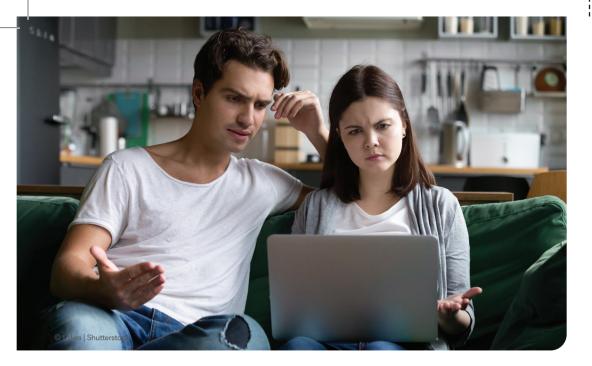
www.nhw.com.au/manningham hello@nhw.com.au

(f) @manninghamNHW



If you can spot a scam, you can stop a scam





Know how to spot a scam

- Suspicious, unexpected email or text message with spelling errors and/or doesn't look right.
- 2. Message telling you to click on something or provide personal information.
- Message offering something at an extremely low price or with unbelievable benefits.
- Someone at the front door insisting that an urgent home repair, e.g., branch removal, needs to be done.
- 5. Somebody pushing you to act quickly.
- 6. If it sounds too good to be true, it is probably a scam.

Protect yourself

STOP! Don't do something silly. Take your time.

Get advice from a relative or frienc before taking any action.

When online

- Never send money or bank details to claim a prize or free products.
- 2. Do not open emails or click on links asking for your banking details. Banks never ask for your banking details in emails. Don't provide banking details in suspicious apps.
- 3. Do not provide your banking information by email.
- 4. Regularly monitor your account transactions.
- 5. Limit the amount and type of personal information you put online.
- 6. Don't advertise your holiday plans online.
- 7. Regularly update your privacy settings.
- If physically meeting a person you have only met online, choose a public space and bring someone you trust.

Check the facts

- 1. Check the company's website or a seller's online profile to confirm an offer is genuine.
- 2. Also check the website to ensure that the telephone number and/or email address is genuine.
- 3. Only download apps from the official Google Play Store or Apple Store.

Be cautious with direct contacts

- Do not click on any link provided in an unsolicited email. Search for the company by name on the internet and use that web address and/or telephone number.
- Do not give out personal information on incoming calls. Call the company back using a publicly available number.

Protect yourself

- If you get a strange random phone call from a person claiming to be a government agent and telling you that you are a suspect, hang up immediately.
- Check a person who says they are a government agent, by contacting the agency directly using the phone number or email address from their website.
- 3. Don't give your personal information to a person you don't know.
- 4. If someone asks you to transfer money over the phone, hang up immediately.
- If you are not sure about certain calls, emails, or information, do not carry out the other person's request. Talk to someone you trust or the police.

What to do if you have been scammed

Act fast to prevent further losses



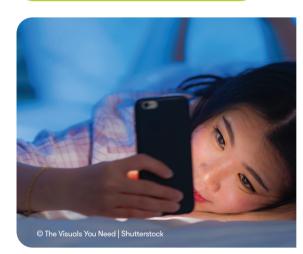
- Contact your bank or card provider immediately to report the scam. Ask them to stop any transactions. Cancel the compromised card(s).
- Get help to recover by contacting IDCARE on 1800 595 160. They can help you make a plan (for free) to limit the damage.
- If your driver's licence, Medicare card, passport or other identity documents have been compromised, replace them.
- If you think you have been a victim of any scam, report it on the website www.cyber.gov.au/report

Tips for people with a Chinese background

Additional scams to watch out for

- A pre-recorded message in Chinese on the phone or social networks (e.g. WeChat, WhatsApp), telling you that your package or valuable item had been seized.
- Threats telling you to transfer large sums of money.
- Demands for money to release a kidnapped person.
- Threats that the authorities will deport or arrest you.

Reporting to the police that you are a victim of a scam, will not affect your visa or residency status.



Additional resources

- Victoria Police police.vic.gov.au/fraud-and-scams
- Consumer Affairs Victoria www.consumer.vic.gov.au/ resources-and-tools/scams/ consumer-scams
- Scam Watch Australian Competition and Consumer Commission www.scamwatch.gov.au