

# Keeping your money safe

Westpac New Zealand



# Financial abuse and scams



# Dating Scams

Be *extremely careful* when you're asked to send money or cards to someone you've met online.

Be concerned if you're only given a post office box and a phone number as contact details.

Be aware of discrepancies in the information you've been told by the other party.

*If it seems too good to be true then it generally is...*



# Job Scams

- Be extremely suspicious of job opportunities that require the use of your bank account.
- If you have received money into your bank account as a result of a job online job offer, do not transfer or access those funds
  - Call your bank's Fraud/Financial Crime team to discuss

*If it seems too good to be true then it generally is...*



# Trading/ Gambling/Shopping Scams

- Be aware of the site's precautions, advice and T&Cs
- Be very cautious trading with overseas-based people who want to pay with Traveller's Cheques, Bank Draft or Foreign Cheque.
- Do an internet search on your buyer or seller, it is common for people to list the names online of people/companies that have duped them.
- Check the Scam Watch website.
- If you think the funds paid to you are linked to a scam, don't access the money and contact your bank's Fraud/Financial Team

*If it seems too good to be true then it generally is...*



# Card Fraud – ATM Skimming

- Maintain your vigilance and regularly check your ATM for any tampering or for anything outside that seems outside of ordinary
- Focus on the green nose and keyboard to ensure it is firm and secure.
- Fraudsters use hidden cameras and watchers. When entering your PIN at an ATM, use your free hand to obscure the keyboard to keep your PIN hidden

*Regularly check accounts*



# Scam Phone Callers

- Be extremely cautious of callers saying they are from the bank, the Police, or any other person/organisation claiming you owe money.
- Call the organisation back on their listed number to confirm.
- Don't provide your personal information. ***Never give you PIN to anyone.***

***Regularly check accounts***



# Identity Theft & Social Engineering

- Keep your contact details up to date with your bank/s.
- Register your mobile phone - set up One Time Verification alerts.
- Secure your home, vehicles and letterbox.
- Limit who can see your social networking information to your friends use the highest security settings available on your site.
- Be careful what personal details and information you post online such as then names of your spouse, children and pets
- Dispose of documents containing personal information like bank statements and bills securely.
- Regularly check your accounts.





# Cyber Crime

- If you think you've received a Westpac-related phishing email forward the email to [phishing@westpac.co.nz](mailto:phishing@westpac.co.nz)
- Do not click on the link contained in the email or log onto your bank's website via a link embedded in emails or 3rd party service.
- Do not reply to the email - delete it.
- Update and perform an anti-virus scan & anti spyware on your computer
- Regularly change passwords, never disclose them to anyone, and always log off your bank's internet site after each session.
- Avoid using public or shared computers
- Select unique passwords, change them regularly.



# Inheritance, lottery & charity scams

- Be extremely cautious when asked to send money to someone you've met over the internet.

Consider:

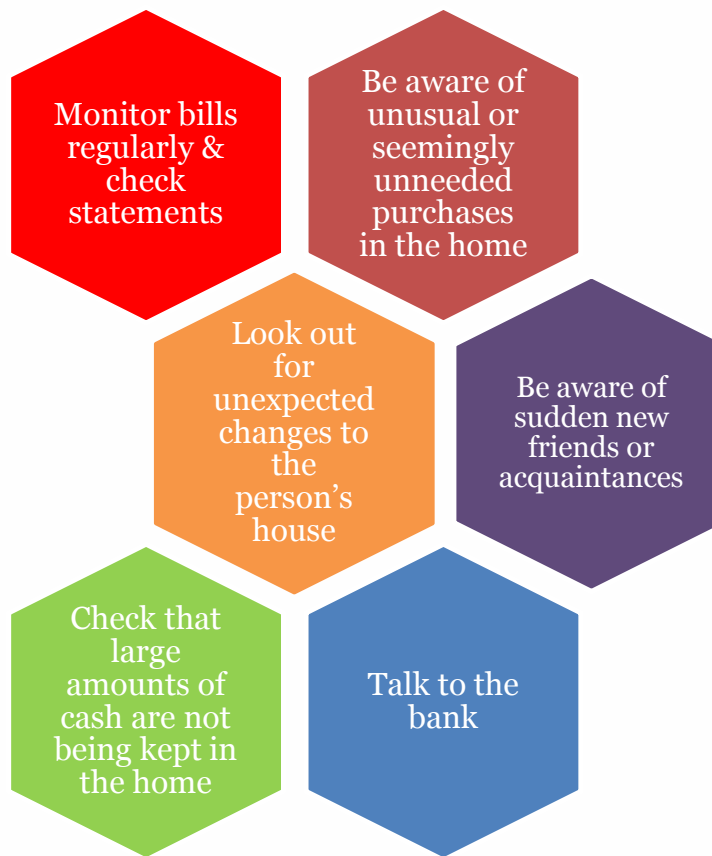
- Do I know about, or have I heard of, the relative, lottery, or the charity?
- How lucky am I considering I did not buy a ticket to the lottery?
- If it is genuine, why do I have to send money to win or inherit money, why don't they just deduct it from the winnings?
- Check the Scam watch and the Charities register.
- Online gambling is poorly regulated and many sites are scams and beware of free trials



# Estate Planning



# Keeping financially safe & signs of financial abuse



# Thank you

