

August 2022: Scams and Frauds

The two guest speakers at our U3A Pegasus 15th August meeting were Mick Myers and Nige Garner from the ANZ bank who gave an enlightening talk on the dangers of scams when using computers for online shopping, banking, and emails. They said there is a 'tidal wave' of scamming currently and their bank saw \$7m of fraud last year. This is up 20% and New Zealanders are easy targets. Forewarned is forearmed, they said.

Phishing is common, mainly emails although they can also be text/SMS messages as well. Messages seemingly genuine from the bank, a business or IRD will ask you to click on a link that will then open you up to a completely different site accessed by the scammer. 80% of scams start from an email. Some will ask you to connect to Team Viewer and all your details can then be accessed. Investment scams offer high rewards, little risk and suggest you are one of the chosen few to get this offer. Romance fraud gets people emotionally snared and then will use various excuses to get you to send money. Identity fraud is dangerous so be careful what information you allow on social media. Mick and Nige particularly referred to Facebook.

Scams usually pressure you to act quickly, not giving you time to think rationally. They ask you to keep things confidential, but request personal information. This usually leads to asking for money, often in increasing amounts. If it sounds too good to be true it's probably a scam.

Mick and Nige had a suite of 'dos' and 'don'ts' which they outlined as central to safety.

- To protect yourself, never give away your PIN or password and create a unique password.
- The longer the password, the more difficult it is to scam.
- Don't respond to unknown emails and,
- Don't send money to anyone you don't know.
- Only shop online with websites you trust. If in doubt get a second opinion.
- Sign any debit/credit card as soon as it arrives and create a different PIN for each.
- Cover your hand when entering your PIN.
- Tell the bank immediately if your card is lost or stolen.

Banks have good anti-fraud measures and can often get your money back if contacted promptly. (They may even phone you to check if you are acting from some place or site that's not usual.)

These websites could be useful:

- www.certnz.govt.nz lists current known non-banking frauds.
- www.idcare.org for ransomware fraud (where your computer is locked down till you pay up.)
- www.netsafe.org.nz for bullying or scams.

.....