NEV2030 Forum Wed 17/4/24
Notes taken by Peter Sniekers (NEV2030)

Scams and Cybercrime

Speakers' presentations - to be read in conjunction with their slide presentations

Ben Fittler (RAB Regional Australia Bank) : Financial Crime Analyst)

- RAB has 38 branches, 100,000 customers and 300 staff.

Rise of the Scambag

Common scams in Australia in order of severity: during 3 months Oct-Dec 2023:

1. Investment scams ($52.4 million)
2. Romance scams ($6.9 million)
3. Employment scams ($4.3 million)
4. Phishing scams ($4.1 million)
5. Other ($10.3 million) **Total: $78 million**

Common delivery methods over same period:

1. Text (25,242)
2. Email (19,900)
3. Phone calls (11,278) (However most money was lost via phone calls).

How to prevent being scammed:

- "PAUSE, VERIFY AND ACT".
  - Pause - Slow down – Stop - there is no rush to act on any advice immediately:
  - Verify through independent sources/advice. Check if they are licensed or not on MoneySmart.
  - Act cautiously: proceed carefully.
  - Don't be afraid to say "NO!" Any push for urgency should be seen as a red flag.
- Watch out for fake invoices and payments and impersonators on-line. Ring up and verbally confirm bank details on any suspect invoices.
- Buy from trusted sources only.
- Avoid paying to a bank account.

Different scams

Impersonations: ATO, Australia Post, banks, telco's, government departments, internet service providers, toll collection agencies. **Never click on any email / text links.**

Romance / relationship scams: meet face to face only, but still beware. Many romance scammers groom victims over the long term

Overpayment scams: can happen on the buy or sell side. Beware.

Investment/ crypto scams: confirm ASIC licensing, speak to any advisor in person and seek independent advice, don't send good money after bad. "If it seems too good to be true, it IS". Don't be trapped by the FOMO affect (fear of missing out). Only invest in what you **understand**. Beware of **Ponzi** schemes.

> **From Investopedia:** "A Ponzi scheme is an investment scam that pays early investors with money taken from later investors to create an illusion of big profits. A Ponzi scheme promises a high rate of return with little risk to the investor. It relies on word-of-mouth, as new investors hear about the big returns earned by early investors".

Smishing or SMS scams: becoming more common but a "trustworthy register" is being developed to reduce number of SMS scams.

Psychology of the Scam

- More social engineering than straight theft (ie. the "grooming" element).
- Preys on stress and exhaustion (eg. Many such phone calls around 6pm).
- Always include a sense of urgency.
- Urges an emotional rather than rational response.
- It is easy to think you are immune.

Become an "expert":

- Learn how to recognise scam attempts.
- Practise secure password management.
- Report suspicious activity.
- Use banking and payment controls.
- Cybersecurity is not a "set and forget" proves.
- Check on-line resources available (see presentations)

Martin Levins (Director - ICT Educators NSW, President - Australian Council for Computers in Education)

Check domain name in web addresses to examine bona fides.

Try phishingquiz.withgoogle.com to see how good you are at recognising scams.

Beware of QR codes: they may be hiding a scam by taking you to a scam site rather than a trusted site.

Use password generators to protect on-line use>

> eg 1Password.com.
>
> Apple and Google Chrome also have password generators built-in.

PWNED: Check if you have been compromised before at:

> Haveibeenpwned.com

Question / Answer session:

Q: Why don't banks know where money has been transferred to?
A: They do, but time is of the essence. Once monies leave the banking system they are untraceable. Banks are more collaborative now than before in detecting and tracing scam transactions

Q: Skimming within scamming?
Eg. Late Telstra bill and then coincidentally receive a scam email saying payment overdue and account to be cancelled if payment not made via a link.
A: If in doubt can always contact client at "security@ domain name": eg security@telstra.com to verify scam or not. By law they need to respond.

Q: Lost $245,000 in an investment scam. Banks not doing enough.
A: In late 2024 there will be an anti-scam code which will make it much clearer around liability surrounding scam transactions.

Q: "Lost mobile" phone scam. What if I did click on a link?
A: Difficult to answer – depends on the operating system you used, if it had been updated at the time etc etc. Important message is DON'T click on any SMS or email link if at all suspect.

Q: Why is there no oversight of domain names to prevent fraudulent web domains being created?
A: There is. However again make sure operating systems / browsers are updated whenever there is any update available on computers / phones / ipads etc to ensure you have the latest security patches.

Q: Purchases on line. I use a debit account and only transfer funds to it when I need to buy on line because I don't like using credit card on line. Some sites however require a credit card or PayPal. Is PayPal secure?
A: Can't answer that quickly but when you use PayPal your credit card details are NOT shared with the merchant so that at least is an extra level of merchant protection. Also easier for refunds if things go wrong. If you are still worried then the debit card method is a good idea.

Statement: audience member had recently been scammed $300 USD on an investment scam but colleagues up to $10,000. She feels Australia is only now playing catch up in the prevention of on line investment scams.

Q: Password generators. Using Norton to generate passwords, but what would happen if Norton is hacked?
A: Would need to contact Norton for their FAQ area and see what they say.

Q: Why did Optus not alert customers their data had been compromised? Overseas they have to!
A: Law has changed. Now once a data breach is detected they are obliged to advise clients and those affected within 30 days.

Q: Email scam from a known person asking for a favour. What if I had replied?
A: Shouldn't be a problem unless they (the scammers) contact you again to ask for any financial information.

Q: Cookies functionality, and by agreeing to "all cookies" am I compromising myself?
A: At one stage nobody was being told what data was being harvested when websites were being visited. Then in Europe legislation was enacted that required users to be told and had to agree to that use. Now that is worldwide. Cookies will tell where you came from to that page, how you got there, what you looked at, considered buying etc. - data is stored on your computer. Then next time you visit that site they can streamline your searches and remind you of previous activity etc. Also reminder emails can be sent to you if you did not close a transaction etc.

In all browsers you can delete all cookies;

and you do not need to accept cookies to use their sites.
Advice: if you use booking engines (eg/ Qantas, booking.com etc). Delete all cookies before going on again because some have suggested they use cookies to determine where you want to go and can affect (increase) the prices they offer.

Statement: Crooks are getting away with scams too easily. It is a case of your privacy and behaviours and data being breached repeatedly. It is "slick robbery" compared to some years ago. Service NSW should have a role of providing better protection.
A/ Yes it is serious, there are many moving parts and makes it even more important to be aware, stay alert and stay up to date.

Speakers were thanked and acknowledged. Main issue is that cyber security is a moving and changing feast and one needs to stay updated to protect themselves on line.
Scammers are very well resourced and trained. Don't get trapped.

Next forum : 4/9/24: Meet the candidates for the upcoming local government elections.