Scam Awareness – Your Best Defence

Charles Fellner (I welcome you contacting me)

charlesfellner1@gmail.com

0409 445 483

Every day we hear about some new scam. As a society we need to be working together a lot more and reaching out to increase our **resilience to scamming**. All it takes is one lapse of judgement and your lifesavings could be gone. We also need to be doing a lot more to reach out to the most vulnerable in our society (e.g. those over 80, with dementia, or disabled) to help and support them through these times where scamming has become rampant.

Down the track, if you do get scammed then, after reporting it to **Scamwatch,** if you wish, you can also contact me and let me know details. I will consider how to use that information to potentially prevent the next person from being caught in a similar scam.

Passwords:

High-Risk online accounts – make sure each is non-guessable and unique :

- Banking/Investment accounts
- Your email
- Your Windows O/S
- any that include your **Medicare number, driver's license,** and/or **passport number**
- any that has your **credit card details** saved
- any containing your personal **medical data**

If you enter your password on a fraudulent site:

- immediately change that password
- where you have reused the same password on other online accounts, change them

Credit/Debit Cards:

Credit/Debit Card Recommendations:

- Use a card with a **small limit** and **no direct debits** for purchases when overseas and also when using any websites that you are not familiar with
- Check your card for fraudulent transactions, at least, **weekly**
- Don't use **public wi-fi** when in airports or shopping centres

If you enter your credit/debit card on a fraudulent site:

- Immediately contact bank concerned and have them shut down your credit card
- Request a new one

Malware:

If malware has been downloaded on your Android phone

- Go to Google and type:
  Remove malware or unsafe software Android then select: "**Google Help**" website

If malware has been downloaded on your laptop

- use anti-virus software to remove it

Helping a relative or friend become more scam resilient:

- Tell them **NEVER** to give out their password or PINs

- Ask them to always know who they are communicating with.
- Ask them not to open suspicious texts, pop-up windows or click on links or attachments in emails
- Ask them not to respond to calls about their computer asking for remote access
- Ask them to keep their personal details secure.
- Ask them to keep their mobile devices and computers secure.
- Suggest they send all mobile calls from an unknown number direct to voicemail
- Ask them to change their social media settings to the strictest privacy controls.
- Encourage them to use 2 Factor Authentication.
- Consider setting up call alerts and monitoring for their bank transactions.
- Consider instigating a permanent credit freeze for them.

Facebook Scams:

To report a fake Profile to Facebook:

- Go to Google and type:
  How to report a Facebook account or Page that's pretending to be me
  … and follow the instructions

Important Facebook privacy settings:

- Date of Birth:
  => Change **Day** and **Month of Birth** to whatever you want, so long as it is NOT **Public**
  => Change **Year of Birth** to **Only Me**
- Who Can See Your Facebook Friends:
  => Change it to whatever you want, just make sure it is NOT Public.

Facebook Marketplace:

- To find out about Facebook Marketplace Scams - go into Google and type:
  18 Facebook Marketplace Scams | All About Cookies

Romance Scams:

The 9 Warning Signs

- You can't find information about them online
- They quickly tell you they love you (i.e., "love bombing")
- Too perfect — especially in photos
- Always traveling or live far away from you
- Refuse to video chat (or always cancel)
- Constant family or personal emergencies
- Asking for financial help or talking about investments
- Pushing for your personal information
- Try to move the conversation off the dating site or app

Investment Scams:

Tips:

- Find the opportunity yourself by doing thorough research
- Seek independent reviews and make sure the investment is legitimate
- Check their AFS license number

- Do not get taken in by high pressure tactics
- Double check all documentation that you receive
- If there is an associated website, check it thoroughly
- Check the investment prospectus is registered with ASIC
- If the returns on offer seem too good to be true be extra vigilant

Large Data Breaches:

- To find what personal details from you are on the dark web as a result of breaches: haveibeenpwned.com

Identity Theft:

Being Ready:

- Be aware of which online accounts have your critical personal data
- List the potential online accounts you are concerned about
- Log into each one and confirm what information they have on you.

In Your Home:

- Protect your laptop with a Windows password or Login password
- Protect your mobile phones with a pin number
- Keep key personal information in a safe place where no one will find it.
  => In visible sight is not a safe place.
- If you have a password notebook => keep it in a safe place

2 Factor Authentication:

- Act Now, Stay Secure–the govt website which explains **2 Factor Authentication** https://www.cyber.gov.au/learn-basics/explore-basics/mfa
- **2 Factor Authentication** Directory – shows which online accounts support 2FA https://2fa.directory/au/

Helpful Online Resources:

- ACCC – **National Anti-Scam Centre** – Scamwatch – for reporting scams https://www.scamwatch.gov.au/
- ACCC – **Little Black Book of Scams** – The Scamwatch main reference document https://www.accc.gov.au/about-us/publications/the-little-black-book-of-scams
- **Australian Cyber Security Centre** – Cyber Security incidents - Scam awareness basics https://www.cyber.gov.au/learn-basics
- **IDCare Learning Centre** – supporting individuals & organisations impacted by recent data breaches & identity theft– free practical and behavioural support https://www.idcare.org/learning-centre
- **Be Connected** – increasing the confidence, skills & online safety of older Australians https://beconnected.esafety.gov.au/topic-library/articles-and-tips/how-to-spot-a-scam
- **NSW Fair Trade Commission** Scams/Cybercrime. Scams related to buying of products https://www.fairtrading.nsw.gov.au/buying-products-and-services/scams
- **MoneySmart.gov.au** – for greater financial wellbeing. Protecting yourself from Scams https://moneysmart.gov.au/online-safety/protect-yourself-from-scams

- **ESafetyCommissioner** – independent regulator – relates to online personal safety https://www.esafety.gov.au/key-issues/staying-safe/online-scams

What To Do If You Have Been Scammed?

Follow the guidelines on Scamwatch which is under the ACCC:

- Go into Google and type:
  Scamwatch what to do if you have been scammed

⇨ Contact your bank(s) or card provider immediately. Ask them to stop any transactions.

Where To Report a Scam?

Report it to Scamwatch:

- Go into Google and type:
  Scamwatch report a scam

Simple Things That You Can Do Today!

1. **Passwords -** Make your passwords for all your high-risk online accounts non-guessable and unique.
2. **Create a scam monthly reminder list for yourself** – you can do this on your iphone in the Reminders app. Here are some reminders to include:
   - **Email/texts Scams** – never open a link or an attachment in an email or text unless you are 100% sure it is legitimate.
   - **Emails** – 'Alteration of Payment Details' – Before you pay a seller the big money, ring them and confirm the bank account
   - **Phone Scams – Call from "The Bank"** – Hang up. Ring them back via the number on the website to confirm.
   - **Phone Scams – Tech Support call from Telstra/Microsoft etc.** – Always fake. Hang up & ignore.
   - **Investment Scams** – Never trust a cold call. Always better to do your own research. Best to find a reputable organisation most of us have heard of.
3. **Identity Theft** – Find a safe place in your house for passports & password books.

To Do – Ongoing

- Always remember these two words when online: **'Be Sceptical'**
- Make scam awareness part of your **daily life**
- Regularly ask the same question to yourself:
  "Is there anything I'm doing that makes me at risk of being scammed?"
- If the answer is "yes", then ask:
  "What changes can I make that can reduce that risk?"
- Then, if necessary, seek assistance first, and then make the necessary changes.
- **Keep talking** about scamming with your friends and relatives

Helpline:

- For all questions regarding scamming, related to scamming, or cyber security incidents you can ring the **Australian Cyber Security Centre** on **1300 292 371**