Scam Awareness – Your Best Defence

Charles Fellner
charlesfellner1@gmail.com
0409 445 483

Every day, we hear about some new scam. As a society, we need to be working together and reaching out to increase our **resilience to scams**. All it takes is one lapse of judgment, and your life savings could be gone. We also need to do 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 when scamming has become rampant.

Down the track, if you do get scammed, then you can report it to:

- **cyber.gov.au/report-and-recover** for reporting a scam with financial loss
- **IDCare** for identity theft and data breach incidents.
- **Scam Victim Alliance** for support in navigating the complex aftermath of a scam.

Passwords/PINs:

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

- Banking/Investment accounts
- Your email account
- All your Windows/Mac/iPhone device & account logins
- Any online accounts that include your **Medicare number, driver's license,** and/or **passport number**
- Any online accounts that have your **credit card details** saved
- Any online accounts containing your **medical data**

If you enter your password on a fraudulent site:

- Immediately change that password
- Then run a security check to ensure no data was compromised.

For ALL your devices:

- Make sure that for each of them, you have to enter a **password/pin** to access them

To check the security of your passwords:

- **For iPhones**: open the "Passwords" app. Then go to Security.
- **For Android phones**: go to Google Password Manager.
  Open Settings → Passwords & Autofill → Google Password Manager → Checkup.
- If you see "compromised," "reused," or "easily guessed," change those passwords immediately.

Blocking Email Senders:

You can use your email app to block senders:

- **Apple Mail**: Swipe left → More → Block Sender
- **Outlook**: **(Classic POP3)**: Open email → copy email address → Settings → Mail → Junk Email → Add Blocked Sender → Enter email address → OK
- **Gmail**: Open email → 3 dots → Block Sender

Payment Methods:

Payment Methods – How safe are they?

- #1 (safest) – PayPal
- then Credit Cards
- then BPay

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 **fortnightly**
- Never enter passwords or pins on **public wi-fi** when in airports or shopping centres

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

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

Malware:

If malware has been downloaded on your:

Mobile Phones (Android):

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

Desktops/Laptops:

- Use your anti-virus software to remove it, or if that doesn't work, then ...
- Go to Harvey-Norman for professional removal.

⇨ If you suddenly realise malware is in the process of being downloaded on your device, then immediately force a shutdown by pressing and holding the power button for 5-10 seconds.

Safe Device Practices:

Recommendations:

- Install updates promptly — they patch security holes.
- Use antivirus software and keep it current.
- Always make sure that you have active anti-virus + VPN (Virtual Private Network) software running on it.
  => Some recommendations: **TOTAL**AV; Norton; bitdefender
- Don't download free "utility" apps (managing, tuning, or optimising software) unless from a trusted store.
- Log out of your high-risk accounts when using devices shared with other people

5 Signs Your Computer Has Been Hacked:

- Your antivirus software has been disabled
- New or strange files show up
- Suspicious logins or alerts on your online accounts
- Your computer is slower than usual
- Your default browser has changed without your permission

⇨ Refer to the following website to resolve these issues: https://scamvictimalliance.org.au/resources/getting-money-back-after-scam-n28k9

Helping the elderly/vulnerable towards scam-resilience:

- 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 to voicemail
- Ask them to change their social media settings to strict privacy controls.
- Encourage them to use 2 two-factor authentication.
- Consider setting up call alerts and monitoring for their bank transactions.
- Consider instigating a permanent credit freeze for them (ref. Barefoot Investor).

Fake Websites:

- Before purchasing from a website, you should check for:
  - misspelled URLs,

- check independent website review and checking services (*e.g.* Fraudr, ScamAdviser, Trustpilot, Feefo)
- look for poor grammar or links that don't go anywhere.

- **HTTPS:** and **websites with a padlock** are lower risk
- You have just entered your credit card details on a fake website. **What should you do?**
  => You should **immediately** contact the bank concerned and have them shut down your credit card

Social Media Scams:

Common tricks include:

- "Tag a friend" competitions that harvest contact lists
- Fake "investment opportunities"
- Malware links disguised as news stories or shocking videos

Facebook: To report a fake Profile:

- Google:
  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 the **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 & posts:
  => Change it to whatever you want, just make sure it is **NOT Public.**

Facebook Investment Advertisements:

- Never click on these. They cannot be trusted.

Facebook Marketplace:

- To find out about Facebook Marketplace Scams - Google:
  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 travelling or living far away from you
- Refuses or cancels video chats (or AI generates them)
- 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
- Check if they have been flagged on the MoneySmart Investor Alert list
- Check that the investment prospectus is registered with ASIC
- Check for scam reports on the Scamwatch database
- If there is an associated website, check it thoroughly
- If the returns on offer are well above the market, be extra vigilant

Data Breaches:

- To find (some of) your personal details on the dark web as a result of breaches: use the **NordVPN** and **Norton360 Deluxe** monitoring feature, or go to haveibeenpwned.com
- To prepare for a potential data breach, you can:
  - Only tell organisations the information that you need to provide services, rather than everything they ask for.
  - Look for organisations that commit to cyber security.

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
- Keep key personal information and password notebook in a safe place where no one can find it.
  => In visible sight is not a safe place.

2 Factor Authentication (2FA):

- For any High-Risk online account with the 2FA option available:
  I strongly recommend toggling 2FA to 'on' as an extra security step.
- Act Now, Stay Secure–the govt website which explains **2FA**
  https://www.cyber.gov.au/learn-basics/explore-basics/mfa
- **2FA** Directory–shows online accounts that 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** – supporting individuals & organisations impacted by recent data breaches & identity theft– free practical and behavioural support
  https://www.idcare.org/learning-centre
- **Scam Victim Alliance –** support, recovery and justice for scam, fraud, and cyber crime survivors.
  https://scamvictimalliance.org.au/
- **Be Unstoppable** – if professional counselling is required after being scammed
- https://www.beunstoppablefoundation.org/
- **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 the 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
  https://moneysmart.gov.au/check-and-report-scams/investor-alert-list
- **Act Now, Stay Secure – the government website that explains 2FA**
  https://www.cyber.gov.au/learn-basics/explore-basics/mfa

- **ScamAware Chatbot** – If you suspect you might be being scammed, this chatbot gives you the likelihood that you are getting scammed based on the information that you provide https://chatgpt.com/g/g-68a8cb67ada88191b604639de5f68499-scamaware

Preparing Yourself Now – Your Checklist

Cyber.gov.au	1300 292 371
IDCare	1800 595 160
Your bank #1	
Your bank #2	
Your Super	

What To Do If You Have Been Scammed?

If you've been scammed:

- **Contact your bank** or **card provider** immediately.
- **Change passwords** for all affected accounts.
- **Run antivirus software** to remove malware.
- **Report it** to provide details of your financial loss
- **Scam Victim Alliance(SVA)** for support navigating the complex aftermath
- **For focused counselling**: **SVA or 'Be Unstoppable'**

Use the following website to try to get your money back after a scam:
https://scamvictimalliance.org.au/resources/getting-money-back-after-scam

Where To Report a Scam?

- **Scamwatch.gov.au** – record and monitor scams
  => report an attempted scam with no loss of money or personal information
- **Cyber.gov.au/report-and-recover** – report online crime
  => report a scam which has resulted in loss of money or personal information
- **IDCARE.org** – data breach, identity theft counselling and recovery help.
- **Your bank or telco** – most now have dedicated fraud teams.

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 five suggested reminders:
    - **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"** – Ask for Customer Reference # => Hang up => Ring 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 that most of us have heard of.
3. **Identity Theft** – Find a safe place in your home for passports, certificates & password books.

To Do – Ongoing

- If you are unsure, then always choose the side of **scepticism.**
- Make scam awareness part of your **daily life**
- Regularly ask the same question of yourself:
  "Is there anything I'm doing that makes me at risk of being scammed?"
- If the answer is "yes", ask: **"What changes can I make to reduce my risk?"** If necessary, seek assistance first, then make the changes
- **Keep talking** about scamming with your friends and relatives

Helplines:

- For all questions regarding scamming, related to scamming, or cybersecurity incidents, you can ring:

Scamwatch	Scamwatch report form.
Australian Cyber Security Centre / Cyber.gov.au	1300 292 371
IDCare	1800 595 160
Scam Victim Alliance	0411 025 866