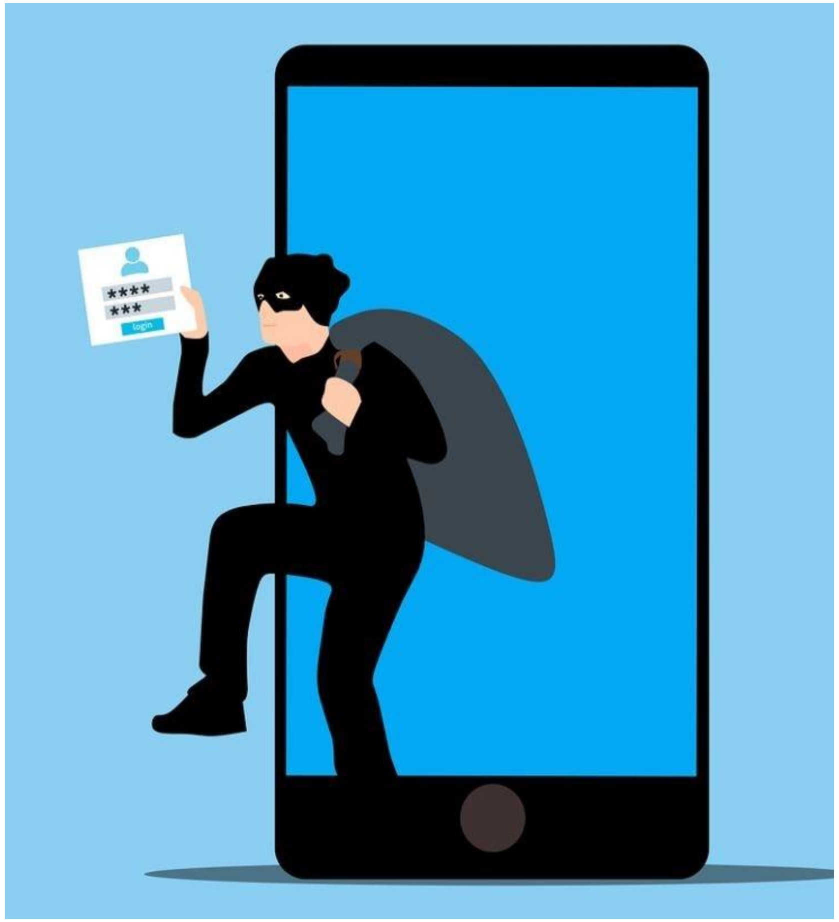


Staying Safe with Technology Online

Final - Version 1.0

Your instructor

- Phil O’Brien
- I am passionate about helping people learn and thus be empowered
- My aim of this presentation is to encourage you to begin or continue on your staying safe journey
- There is not enough time to deep dive on all concepts presented but you will learn how to find out further information
- During question time, the only stupid question is the one that you do not ask

Disclaimer:

- One or more generalisations may be made to simplify explanation of a concept.

Key Take-Away for this presentation

- **Be Aware not Afraid**

- It is all about reducing the risk of being adversely impacted
- Like building a house, security is built up in stages, so will your level of safety
- Learn where to find information that will help you
- Become more confident on how to protect yourself.

Scams in general

- There are many categories of scams. Some scams are face to face or phone and others are via your devices (phones, computers, tablets). A partial list of scams is:

Dating & Romance – build up trust then ask for money

Investment – Offer better returns

Unexpected Money – Unexpected inheritance

Prize & Lottery - Just give me some money for taxes Online

shopping – Wow – how cheap is that!

Identity theft – Data leakage leading to you being impersonated

Job / employment

Charity and medical scams ….. And the list goes on.

How scams work

- Scammers typically try and get your hard earned $$$
- They may use personal data 'Hello, can I speak to Phil O'Brien?'
- They may contact you multiple times to build up a sense of trust
- They may play with your emotions
- Scammers try to get you to panic so that you do not think clearly
- They may use high pressure sales tactics
- They may replicate a family member's voice.

Potential impacts of being unsafe

- Increased anxiousness / loss of confidence
- Loss of money or no longer able to access your money
- You regular payments being redirected to some one else
- Payments you normally receive, cease
- You are impersonated (identity theft) and loans are taken out in your name for which you are liable
- Your accounts are used for illegal activities and you are inconvenienced by the investigation due to your account being frozen.

Potential impacts of being unsafe - continued

- No longer able to access critical services such as government services, medical scripts and more
- Miss out on the opportunity to buy something at a reduced price due to your device not being available
- Miss out on an important medical appointment, due to reminders not working
- Unexpected costs due to needing technical support (usually $80 to $120 per hour) to recover your device, if possible
- Slowing down of your device to the point it is frustrating to use
- Your devices crashes (stops working).

What can I do to reduce the risk?

- Understand the basics. If it is too good to be true, it is !!!
- Know where to look up information that may assist you
- 'The Little Book of Scams' – types of scams, identifying the scam, avoiding the scam, what to do if you have been scammed
- The book can be downloaded from the Australian Competition & Consumer Commission for free: https://www.accc.gov.au/system/files/little-book-of-scams-2024english.pdf
- Don't be rushed. Speak to a trusted advisor and / or friends
- Other publications will be referenced later in the presentation.

High Level steps to undertake

- Good password management – Use a Password Manager
- Two Factor Authentication
- Use of Biometrics (finger print / face id)
- Keep your device up to date
- Regular backups of your data
- Don’t click on links
- Understand your device
- Verify details from official web sites.

High Level steps to undertake

- Perform checks to see if an email is valid – Check senders name against their email address.   This is just one of the checks
- Use email filtering for people who are sending you junk email or trying to scam you.   Automatically delete scam emails
- Avoid public Wi-Fi entirely especially if banking or shopping unless using a Virtual Private Network (VPN)
- Use Bookmarks in your Browser.   Ensure you are going to correct site
- Only download apps / programs from official stores and websites
- Take action on recommended tasks from your device
- Dispose of paper bills securely.

Passwords – What to do and not to do

- Use the right mix of characters. A-Z, a-z, 0-9, and symbols such as $
- How secure is my password https://www.security.org/how-secure-is-my-password/
- Do not repeat passwords
- Do not use similar passwords
- Do not use words that are in the dictionary
- Do not use information that can be determined online or is available publicly.

Passwords – Continued

- Do not take a photo of your passwords
- Do not store your password electronically unless in a Password manager
- Do not share passwords via email
- Do not write down your passwords
- Do not use a password that has been leaked
- Do not use a Master Password (keys into a Password Vault) for a site.

Password Manager - Features

- Only need to remember one password
- Auto completes forms on websites for recognised sites
- You can add secure notes
- Generate strong unique passwords
- Synchronise your passwords across devices
- Near real time notification of data breaches.

Password Manager - Features

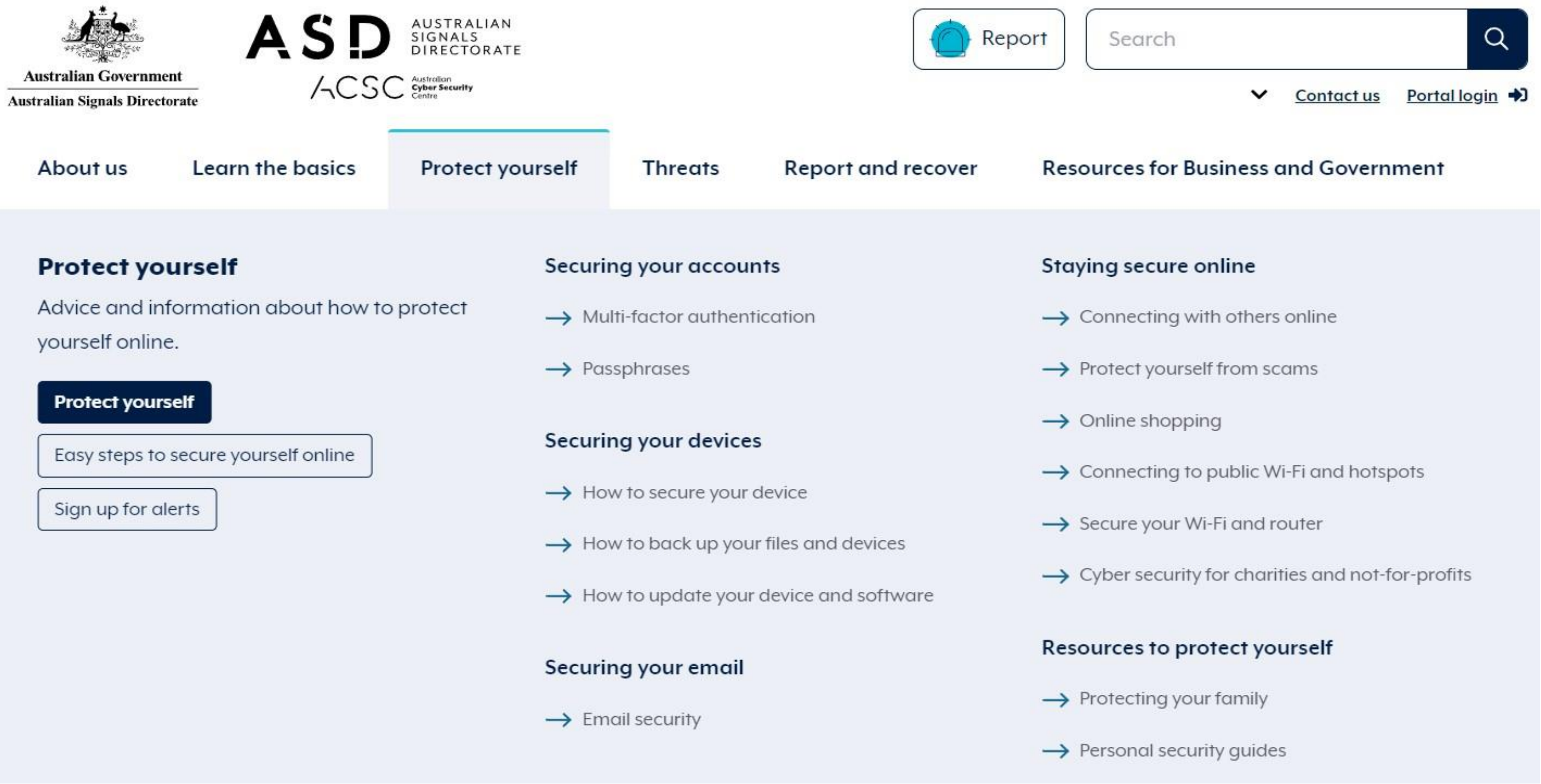
- Report on weak and duplicate passwords
- Inclusion of Virtual Private Network
- Ability to share passwords securely (if you must).

Have my details been leaked

- Leaked details could be email address, password, drivers license, address, account numbers and more
- Criminals build up the details until they can impersonate you or sell your details to other criminals
- How do I know what details are leaked and when? Free website https://haveibeenpwned.com/
- Change affected passwords
- Check financial records, not just balances.

Australian Government – Official Home Page

- https://www.cyber.gov.au/


Australian Government
Australian Signals Directorate
ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre
Report
Search
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government

Protect yourself

Advice and information about how to protect yourself online.

Protect yourself

Easy steps to secure yourself online

Sign up for alerts

Securing your accounts

- → Multi-factor authentication
- → Passphrases

Securing your devices

- → How to secure your device
- → How to back up your files and devices
- → How to update your device and software

Securing your email

- → Email security

Staying secure online

- → Connecting with others online
- → Protect yourself from scams
- → Online shopping
- → Connecting to public Wi-Fi and hotspots
- → Secure your Wi-Fi and router
- → Cyber security for charities and not-for-profits

Resources to protect yourself

- → Protecting your family
- → Personal security guides

Useful link – Personal Security Guides

- Top tips for staying safe online

  https://www.cyber.gov.au//sites/default/files/2023-07/2023_ACSC_Top%20tips%20for%20cyber%20security%20poster%20A4.pdf

- Be Connected – lots of good articles – typically less than 8 minutes to read.   Good use of everyday language.

  https://beconnected.esafety.gov.au/topic-library?cfp_multiselect_subjectsubject_9902b[]=Safety&orderbykey=featured&itemstyle=narrow