Maintaining Cyber Security

Helpful websites:

- Australian Government - Department of Home Affairs
- Australian Federal Police - Cybercrime
- Australian Signals Directorate - Cyber Security Centre (ACSC)

Cybercrime is often linked to:

- drug crime
- fraud and corruption
- money laundering and financial crime
- serious and organised crime.

Different forms of cybercrime include:

- malware, such as remote access trojans (RATs), keyloggers and ransomware, which inserts a file or code to infect, explore or steal information over a network
- phishing and spear (targeted) phishing, such as fake emails from a bank asking for login details
- man-in-the-middle attacks, where the attacker secretly relays and possibly alters communications between 2 parties who believe that they are directly communicating with each other
- SQL injection, a common web-hacking technique that adds malicious code to a database.

Email Breach's

If someone, is accessing and using another person's email account to impersonate them, this is considered unauthorised access and can be a criminal offence in Australia. Here's how you can report it:

1. Confirm it's truly unauthorised

- As email account owner you will know, or Speak to the owner directly to confirm
- Gather any evidence (emails, timestamps, headers) that show the impersonation.

2. Report to the email provider

- Forward the impersonating emails (with full headers) to the provider's abuse team.
- For Gmail: abuse@gmail.com
- For Outlook/Hotmail: abuse@outlook.com
- For other providers, search "report abuse [provider]".
- State clearly: "The account owner has not authorised this person. They are impersonating the owner and sending fraudulent communications."

3. Report to the Australian Cyber Security Centre (ACSC)

- Submit a report at cyber.gov.au/report.
- Choose ReportCyber and select "Unauthorised access / identity theft".
- Attach evidence (emails and headers).

4. Police involvement (if required)

- If the impersonation is used for fraud, threats, or causes serious harm, lodge a report with your local police.
- Take printed copies of the emails and the ACSC report reference number.

5. Secure the email account

- Change the email password immediately.
- Remove any recovery addresses or forwarding rules that you may have set up.
- Enable two-factor authentication (2FA).

Important:

- Family member impersonation is still illegal and classed as identity theft/unauthorised access under the Criminal Code Act 1995.
- Reporting via ReportCyber ensures the case is directed to the appropriate police jurisdiction in Australia.

Practical Guidance

1. Email to the email provider (abuse team)

Subject: Unauthorised Access & Impersonation – [Email address]
To: abuse@[provider].com

Body:
Dear Abuse Team,

I am the owner of the email account [email address]. I have discovered that someone is accessing this account without my permission and is impersonating me by sending emails and signing off as me.

This is unauthorised access and identity impersonation. Please investigate and secure my account immediately.

Evidence:
- Emails attached showing the impersonation (with full headers)
- Dates/times of suspicious access

I request that any unauthorised sessions be terminated and the account be secured. I have now changed the password and enabled two-factor authentication.

Please confirm receipt and advise on any further steps required.

Kind regards,
[Full name]
[Contact phone number]

2. Report to the Australian Cyber Security Centre (ACSC)

Go to: cyber.gov.au/report

- Select ReportCyber → "Unauthorised access / identity theft".
- Include:
  - A summary of the situation.
  - The son's name and relationship (if known).
  - Dates/times of impersonation.
  - Attach the same email evidence.

3. Police Report (if necessary)

If fraud, threats, or harm is involved, go to your local police station and provide:

- Printed copies of the impersonating emails (with full headers).
- The ACSC report reference number.
- Evidence that you own the account (e.g. account recovery email from provider)

4. Immediate Account Security Steps

- Change the email password to a new strong password (not previously used).
- Remove any backup emails or phone numbers you don't recognise.
- Remove forwarding rules (check Settings → Forwarding & POP/IMAP).
- Enable two-factor authentication (2FA).