Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Annual Cyber Threat Report 2024–25 fact sheet

For individuals

Individuals are commonly targeted by cybercriminals for financial gain. This can be through scams or through the on-selling of personally identifiable information or usernames and passwords online.

State-sponsored cyber actors have also compromised home devices connected to the internet, such as home routers, to create botnets that support further targeting around the globe.

Every Australian can take steps to protect their most valuable assets and significantly reduce personal risks while engaging technology.

Cyber threat facts for 2024–25

In FY 2024–25, Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) received over 84,700 cybercrime reports, one every 6 minutes.

The average self-reported cost of cybercrime for individuals has risen in FY2024–25 to $33,000 (up 8%).

Queensland, Victoria and New South Wales report more cybercrime than any other state or territory, with disproportionately higher reporting rates relative to their populations.

The **top 3** self-reported **cybercrime** types for **individuals** were:

- Identity fraud **(30%)**
- Online shopping fraud **(13%)**
- Online banking fraud **(10%)**

Annual Cyber Threat Report 2024–25 fact sheet

For individuals

Take action to protect yourself and your family

Be aware

Understand the risks that could impact you.

Identity fraud involves cybercriminals using another individual's personal information without consent, often to obtain financial benefit.

Online shopping fraud is when cybercriminals target online shoppers to steal their money or their personal details.

Online banking fraud can occur when cybercriminals gain access to an individual's online banking account through their details, this can lead to unauthorised account transactions.

Get active

Strong cyber security starts at home. Begin with the basics:

- Use phishing-resistant multi-factor authentication wherever possible, preferably passkeys.
- If you use passwords or passphrases, make them strong and unique, and consider using a reputable password manager.
- Keep software on devices updated, and only use a trusted device when accessing sensitive online accounts. For example, use your bank's app on your smartphone to perform internet banking.
- Be alert for phishing messages and scams.
- Regularly back up important files and device configuration settings.

More Information

If you own or operate a business or organisation in Australia, check out our ***Annual Cyber Threat Report 2024–25 fact sheet for businesses and organisations*** and stay up to date on the cyber threats to businesses. Read the full report and find the latest cyber security advice and a range of practical how-to guides on cyber.gov.au.

It is critically important that individuals who see suspicious cyber activity, incidents and cybercrimes report to ReportCyber at cyber.gov.au/report.