



# 2023–2024 Cyber threat trends For individuals

- Over 87,400 cybercrime reports were made in FY2023-24, a decrease of 7% from the previous financial year, an average of one report every 6 minutes.
- Answered over 36,700 calls to the Australian Cyber Security Hotline, an average of 100 calls a day, an increase of 12% from FY2022-23.
- The top 3 cybercrimes reported by individuals were:
  - identity fraud (26%)
  - online shopping fraud (15%)
  - online banking fraud (12%).
- The average self-reported cost of cybercrime per report for individuals increased to around \$30,700 (up 17%).
- According to the Australian Institute of Criminology's *Cybercrime in Australia 2023 report*, 34% of respondents had their financial or personal information exposed in a data breach in the 12 months prior to the survey. Of these, 79% were notified by the company whose data was leaked or by a government or financial agency.

Cyber threats are rapidly evolving. The average Australian household has 12 or more devices connected to the internet, and are spending more time online than ever before.

The main cyber threats to watch out for include:

- **identity fraud** - when someone pretends to be you and uses your personal information to steal money or make fake accounts
- **online shopping fraud** - illegal activities or scams that occur when shopping on the internet, and
- **online banking fraud** - when cybercriminals gain unauthorised access to your accounts leading to the theft of money, sensitive information or unauthorised transactions.

Cybercriminals often use phishing scams to impersonate real businesses and get you to click on malicious links or files. Once you click on a malicious link or file, you may be prompted to provide information, like a password, or malware may infect your device.

Every Australian should continually evolve their cyber security practices to protect themselves and their families from these cyber threats. Some of the most effective ways to protect yourself online are also the easiest to use, fastest to set up and often free.

## **What should individuals do?**

Adversaries evolve and so does cyber security. Good cyber security is not set and forget.

To mitigate against common cyber security threats, you should:

- enable multi-factor authentication (MFA) for online services, when available.
- use long and unique passphrases for every account – password managers can assist keeping track of each password.
- turn on automatic updates for all software (including mobile apps) and do not ignore update prompts.
- backup important files and device configuration settings regularly.
- be alert for phishing messages, calls and scams. If you are unsure, call the official phone number of the organisation to check.

Find the latest cyber security advice and a range of practical how-to guides on [cyber.gov.au](https://www.cyber.gov.au).

Report cyber security incidents and cybercrimes to ReportCyber at [cyber.gov.au/report](https://www.cyber.gov.au/report).

Together we can make Australia the most secure place to connect online.