Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

2022–2023 CYBER THREAT TRENDS
FOR INDIVIDUALS

Nearly **94,000** cybercrime reports, an **increase of 23 per cent** from the previous financial year.

A cybercrime is reported **every 6 minutes**, on average.

Answered over **33,000** calls to the **Australian Cyber Security Hotline** an average of **90 calls** a day, an **increase of 32 per cent** from the previous financial year.

2022–2023 CYBER THREAT TRENDS
FOR INDIVIDUALS

Top 4 cybercrime reported by **individuals** included:

1. identity fraud
2. online banking fraud
3. online shopping fraud
4. investment fraud.

The Australian Competition and Consumer Commission's ***Targeting Scams*** report revealed Australians **lost** over **$3 billion** to scams in 2022.
This is an **80 per cent increase** on total losses recorded in 2021.

The Australian Institute of Criminology's ***Cybercrime in Australia 2023*** report found that **two-thirds** of respondents said they had been a **victim** of at least one type of cybercrime during their lifetime.

2022–2023 CYBER THREAT TRENDS
FOR INDIVIDUALS

The average Australian household now has over a dozen internet-connected devices and we are spending more time online than ever before. In our increasingly tech-driven lives, we use devices and accounts every day that are vulnerable to cyber threats.

Cybercrime is a multibillion dollar industry and there are people out there who may try to trick you through scams and fraud, or by stealing and selling your highly sensitive personal information. It's crucial to be aware of common cyber threats.

The main cyber threats to watch out for include identity fraud and online banking fraud. Identity fraud is when someone pretends to be you and uses your personal information to steal money or make fake accounts. Online banking fraud occurs when cybercriminals gain unauthorised access to your accounts leading to the theft of money, sensitive information or unauthorised transactions.

Cybercriminals often use phishing techniques to steal sensitive information. Phishing messages attempt to trick you into clicking on malicious links or attachments. Once you click on a malicious link or file, you may be prompted to provide private information, like a password, or malware may run on your device.

Every Australian should adopt basic cyber security practices to help 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 and fastest to set up.

What should individuals do?

- Enable multi-factor authentication (MFA) for online services when available. MFA is a multi-step account login process that requires two or more factors of authentication in addition to a password.
- Use long and unique passphrases for every account. A passphrase uses four or more random words, and password managers can assist with creating passphrases to help protect your accounts.
- Turn on automatic updates for all devices and software. Do not ignore installation prompts.
- Regularly backup important files and device configuration settings.
- Be alert for phishing messages and scams.

Visit cyber.gov.au for the latest advice including a range of practical guides for all Australians that explain how to protect your information and devices online.

Report cybercrimes early via ReportCyber at cyber.gov.au/report. For cyber security advice and assistance call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).
The hotline is available 24 hours a day, 7 days a week.

Want to stay up-to-date? Join ASD's Cyber Security Partnership Program as a Home Partner to receive timely cyber security information to protect your information and devices.