Australian Government
Australian Signals Directorate

ASD Australian Signals Directorate
ACSC Australian Cyber Security Centre

cyber.gov.au

2023–2024 Cyber threat trends For businesses and organisations

- 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 businesses:
  - email compromise resulting in no financial loss (20%).
  - online banking fraud (13%).
  - business email compromise (BEC) fraud resulting in financial loss (13%).
- The average self-reported cost of cybercrime to businesses decreased by 8% overall.
  - $49,600 for small business (up 8%).
  - $62,800 for medium business (down 35%).
  - $63,600 for large business (down 11%).
- Almost $84 million in losses due to BEC were self-reported to ReportCyber. BEC continues to significantly impact businesses, with an average financial loss of over $55,000 for each confirmed incident.
- ASD responded to over 1,100 cyber security incidents. 11% of all incidents responded to included ransomware, a 3% increase from last year.

The cyber threat to businesses is constantly evolving. Australian businesses that hold either customer data or proprietary knowledge, make attractive targets for cybercriminals.

The most common cyber threats to watch out for include:

- online banking fraud
- email compromise, and
- business email compromise fraud.

Phishing is a common method used to compromise emails and commit fraud against businesses. Phishing usually takes the form of untargeted, mass emails that may ask for sensitive information or encourage victims to open an attachment or visit a fake website. Phishing can also be in the form of SMS messages and QR codes.

What should Australian businesses and organisations do?

Adversaries evolve and so does cyber security. Good cyber security is not set and forget. We regularly update and improve our guidance as threats evolve.

To mitigate cyber security threats, businesses and organisations should:

- treat a cyber incident as a 'when' not an 'if' – have a cyber security incident response plan and test it regularly with your staff to ensure an effective response and fast recovery.
- ensure products and services are secure-by-design and secure-by-default.
- follow best practice cyber security – adopt ASD's Essential Eight, which is evolving to address new threats and mitigations.
- enable multi-factor authentication (MFA), when available.
- use long and unique passphrases for every account – password managers can assist with such activities.
- turn on automatic updates for all software – do not ignore update prompts.
- backup important files and device configuration settings regularly.
- be alert for phishing messages and scams. Ensure staff are trained to identify phishing messages and scams.
- stay engaged with cyber security – whether you're an individual or an enterprise. ASD's ACSC Cyber Security Partnership Program offers free easy-to-follow cyber security advice for all Australians.

For more cyber security advice, visit the Resources for Business on cyber.gov.au. ASD encourages every business and organisation that detects suspicious activity, incidents and vulnerabilities to report them to ReportCyber at cyber.gov.au/report or by calling the Australian Cyber Security Hotline 1300 CYBER1 (1300 292 371).

ASD's ACSC provides free technical incident response advice and assistance, 24 hours a day, 7 days a week.