Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

2022–2023 CYBER THREAT TRENDS
FOR AUSTRALIAN BUSINESSES AND ORGANISATIONS

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 AUSTRALIAN BUSINESSES AND ORGANISATIONS

Top 3 cybercrime reported by **businesses**:

1. email compromise
2. business email compromise fraud
3. online banking fraud.

The average self-reported **cost of cybercrime** to **businesses increased** by **14% per cent**.

- **$46,000** for **small business**
- **$97,200** for **medium business**
- **$71,600** for **large business**

Almost **$80 million** in **losses** due to **business email compromise fraud** was self-reported to **ReportCyber**.

Business email compromise fraud continues to significantly impact businesses, with an average financial loss of **over $39,000** for each incident.

2022–2023 CYBER THREAT TRENDS

FOR AUSTRALIAN BUSINESSES AND ORGANISATIONS

The **professional, scientific** and **technical services** sector **reported** the highest number of **ransomware-related cyber security incidents** through **ReportCyber** in 2022–23, followed by the **retail trade** sector, then the **manufacturing** sector.

These **3 sectors** accounted for approximately **a third** of **ransomware-related cyber security incidents**.

ASD **responded** to **over 1,100** cyber security incidents. **Ransomware** comprised over **10 per cent** of all incidents, similar to the previous financial year.

2022–2023 CYBER THREAT TRENDS
FOR AUSTRALIAN BUSINESSES AND ORGANISATIONS

Malicious cyber activity is a real risk to Australia's security and prosperity. Many Australian businesses, including small and medium businesses, hold sensitive and valuable information making them an attractive target for cybercriminals.

The most common cyber threats to watch out for include email compromise and business email compromise fraud. The difference between email compromise and business email compromise fraud is that there is a financial loss recorded with business email compromise fraud.

Malicious cyber actors often exploit unpatched and misconfigured systems, or take advantage of weak or re-used credentials to access systems and networks. Analysis undertaken by ASD's ACSC found that half of the vulnerabilities analysed were exploited within two weeks of a patch or mitigation advice being released.

Businesses should patch, update or mitigate vulnerabilities in online services and internet-facing devices within 48 hours when vulnerabilities are assessed as critical by vendors or when working exploits exist. Otherwise, vulnerabilities should be patched, updated or otherwise mitigated within two weeks.

To defend against email attacks, set aside time for regular cyber security training, and ensure staff are cautious of emails that contain requests for payment or change of bank details, or contain an email address that doesn't look right.

If staff receive suspicious emails, they should verify the legitimacy of suspicious messages via the organisation's official website or verified contact information. Contact details that were sent as part of a message should not be trusted, as these could be fraudulent.

What should Australian businesses do?

- Turn on multi-factor authentication for online services.
- Use long and unique passphrases for every account. Password managers can assist with creating passphrases to protect your account.
- Turn on automatic updates for all software, and do not ignore installation prompts.
- Regularly back up important files and device configurations settings.
- Be alert for phishing messages and scams.
- Only use reputable cloud service providers and managed service providers that implement appropriate cyber security measures.

- Regularly test cyber security detection, incident response, business continuity and disaster recovery plans.
- Review the cyber security posture of remote workers including their use of communication, collaboration and business productivity software.
- Train staff on cyber security matters, in particular how to recognise scams and phishing attempts.
- Get the latest cyber security insights and access to the experience, skills and capability of thousands of other Australian organisations by joining ASD's Cyber Security Partnership Program as a Business or Network Partner.

For more cyber security advice, see ASD's resources for businesses at cyber.gov.au, where you'll find ASD's guidance on its Essential Eight Mitigation Strategies and the *Small Business Cyber Security Guide*, plus more practical and easy to follow cyber security advice.

Report cyber security incidents early to 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.