Bulletin

Industry Divisions

Reference No. Cyber Safe 2024/jk-12-23 **Date:** 07/12/2023

Stay Cyber Safe in 2024

Dear member

You would be aware of the inherent cyber security threats all businesses face daily. The risk of an attack has the potential to completely ruin your business, which is why it is important to ensure you have the necessary safeguards in place. Small businesses are particularly vulnerable to cyber risks due to limited resources, infrastructure and a lack of awareness. Unfortunately, the VACC has received calls from members who have been compromised from clicking on suspicious emails, using easy to decipher passwords, and from using software without the critical updates being installed.

The latest report produced by the Australian Cyber Security Centre (ACSC) shows there were nearly 94,000 reports in the 2022-23 period up by 23 per cent on the previous year. On average, the cost to small businesses is $46,00, to medium sized businesses $97,200, and large sized businesses $71,600 per cyber-attack.[1] Victoria is the second highest state, behind Queensland, for reported incidents.[2]

Highest on the list of cybercrimes affecting individuals include: identity fraud, online banking fraud, and online shopping fraud, while for businesses: email hacking and online banking are the main security risks.

The Australian Signals Directorate (ASD) has published guides tailored for individuals as well as small, medium and large businesses. You can access these guides by taking this link.

What you can do to protect yourself:

- enable multi-factor authentication (MFA) for online services where available
- use long, unique passphrases for every account if MFA is not available, particularly for services like email and banking (password managers can assist with such activities)
- turn on automatic updates for all software – do not ignore installation prompts
- regularly back up important files and device configuration settings
- be alert for phishing messages and scams
- sign up for the ASD's free Alert Service.

What you can do to protect your business:

- 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
- implement relevant guidance from ASD's Essential Eight Maturity Model, Strategies to Mitigate Cyber Security Incidents and Information Security Manual
- join ASD's Cyber Security Partnership Program
- report cybercrime and cyber security incidents to ReportCyber.

For more information please visit: https://www.cyber.gov.au/

John Khoury
Industry Policy Advisor

---

[1] Australian Signals Directorate '*ASD Cyber Threat Report 2022-2023*' <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>.

[2] Ibid.