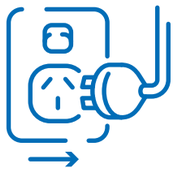
First published: 6 July 2026

Defending against AI-enabled cyber attacks: Guidance for medium-sized businesses

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has developed this guidance to help medium-sized businesses defend against cyber attacks that involve the use of artificial intelligence (AI). Hackers may use AI to rapidly discover and exploit vulnerabilities - especially in internet-facing services such as websites, target many victims at once, and rapidly progress an attack from initial compromise to data theft or extortion.

Recommended actions - immediate

Discuss this guidance with the CEO, cyber security and IT personnel, and cloud and managed service providers.



Regularly identify internet-facing services, such as website servers and email servers, and remove those that are not necessary.

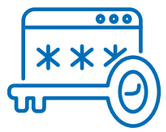
Remove or replace internet-facing services that do not receive security patches (or security updates) from their vendors.

Rapidly apply all security patches (or security updates) for internet-facing services, applied automatically if the risk of a faulty patch is low.

Configure web browsers and operating systems on user computing devices to automatically apply security patches (or security updates).

Recommended actions - short-term

Prepare and exercise plans to remediate cyber security incidents, including restoring from backups that are recent, tested, and protected from unauthorised access, modification and deletion.



Prepare and exercise plans to continue business operations during cyber security incidents, including testing the ability to rapidly block network traffic and reset all user passwords.

Block unnecessary network communication between each internet-facing service, and between internet-facing services and other corporate computing devices.

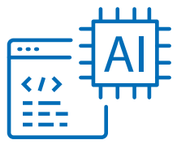
Securely configure internet-facing services to run using an account with the minimum privileges required, and disable or remove unnecessary functionality and insecure settings.

Promptly review security logs from internet-facing services to identify and respond to cyber security incidents.

Recommended actions - medium-term

For internet-facing services, consider using software-as-a-service cloud services that are rapidly patched by reputable cloud service providers.

Choose vendors that develop securely designed software with minimal vulnerabilities, and securely provide adequately-tested patches rapidly after vulnerabilities are identified.



Use AI carefully (in a secure, controlled and human-supervised manner) to find and confirm vulnerabilities in code you build for internet-facing services.

Use AI carefully to assist with analysing security logs from internet-facing services, and performing penetration tests and vulnerability assessments of internet-facing services.

Consider which other corporate computing devices would benefit from timely patching, use of least privilege accounts, secure configuration, and prompt analysis of security logs.