First published: 6 July 2026

Defending against AI-enabled cyber attacks: Guidance for small businesses

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has developed this guidance to help small 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 websites, target many victims at once, and rapidly progress an attack from initial compromise to data theft or extortion.

Recommended actions for small businesses

Share this publication within your business to raise their awareness of AI-enabled cyber attacks.

Turn off your websites that you no longer need, and disable features that you don't need for your remaining websites.

Turn on automatic security patches/updates for computers, tablets and mobile phones used by employees, especially for web browsers and operating systems.

Review which companies you use to store and share your customer data and other sensitive data, and consider changing if they don't take cyber security seriously[1].

If your business develops software, especially for websites, use a process for quality assurance including scanning your developed software for vulnerabilities.

Identify a person or service provider that is responsible for maintaining the cyber security of your websites. Ask them:

- Is the software used by my websites supported by vendors that provide security patches/updates? If not, can you replace it with software that is?
- Are all security patches/updates applied to the software used by my websites, automatic or rapidly applied after becoming available?
- Is the software used by my websites made by a reputable company, and securely configured to disable unnecessary functionality and insecure settings?
- If my websites get hacked, how quickly would you notice and inform me, and can you fix the issue, evict the hacker, and restore from a recent secure backup?

[1] Questions to ask managed service providers https://www.cyber.gov.au/business-government/supplier-cyber-risk-management/managed-service-providers/questions-to-ask-managed-service-providers