

# Cyber security checklist for small businesses

## Secure your accounts

- Turn on multi-factor authentication wherever possible, starting with your most important accounts.
- Use a password manager to create and store unique passwords or passphrases for each of your important accounts.
- Limit the use of shared accounts and secure any that are used in your business.
- Ensure each user can access only what they need for their role.

## Protect your devices and information

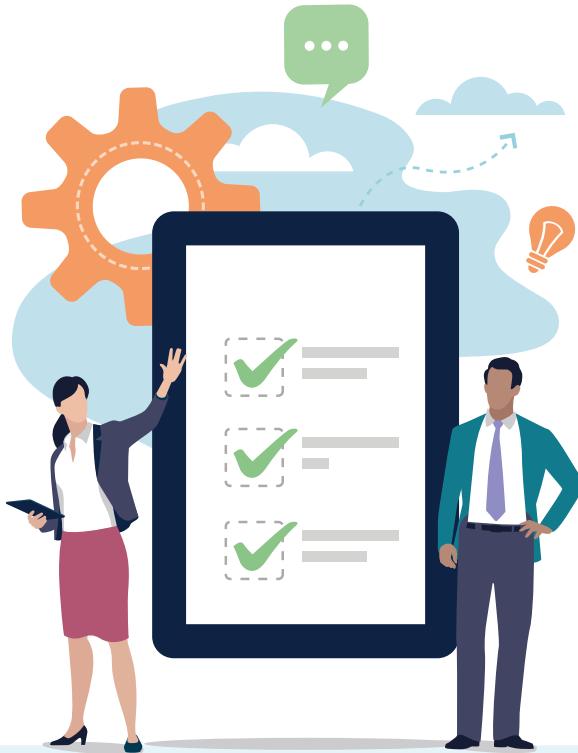
- Turn on automatic updates for your devices and software.
- Create and implement a plan to regularly back up your information.
- Set up security software to complete regular scans on your devices.
- Speak to an IT professional about ways to secure your network.
- Read through the Australian Cyber Security Centre (ACSC) resources on [website security](#).
- Perform a factory reset before selling or disposing of business devices.
- Configure devices to automatically lock after a short time of inactivity.
- Understand the data your business holds and your responsibilities to protect it.

## Prepare your staff

- Educate employees and determine how cyber security awareness will be taught in your business.
- Create an emergency plan for cyber security incidents.
- Register your business with the ACSC Partnership Program.

After completing this checklist, we recommend small businesses implement Maturity Level One of the [Essential Eight](#).

If you have questions about this advice or cyber security more broadly, we recommend you speak to an IT professional or a trusted advisor.



Find out more at [cyber.gov.au/smallbusiness](https://cyber.gov.au/smallbusiness)

**Report cyber security incidents:** [cyber.gov.au](https://cyber.gov.au) | 1300 CYBERI (1300 292 371)



Australian Government  
Australian Signals Directorate

ACSC Australian  
Cyber Security  
Centre