ACSC Australian Cyber Security Centre

Easy steps to secure your online information

Taking these cyber security steps will help reduce the chance that your digital information is accessed by hackers.

Secure your email, social media and apps

Put strong security on important accounts where you exchange personal or sensitive information such as email, bank and social media accounts.

- Turn on two-factor authentication on your important accounts for an extra layer of security.
- Use strong passwords on your accounts — use a passphrase of at least 13 characters made up of about four words meaningful to you but not easy to guess.
- Don't use the same password on any of your accounts.
- Consider using a reputable password manager.

Watch out for scam messages

Online scams and "phishing" by email, SMS, social media posts and direct messaging are designed to steal your logins, credentials and personal details or to download malicious software onto your device.

- Check before you click links — hover over the link to see the actual web address.
- Never enter your username or password from links in messages to your accounts – go to the official website or app.
- If a message seems suspicious, contact the person/business through a separate, legitimate source to confirm it.

Secure your mobile and computer

- Always use a PIN or password on your mobile and computer.
- Always do the software updates such as Microsoft, iOS and Android.
- Make sure you download apps from official stores.
- Install security software on your devices to protect you from malicious software.

Check public Wi-Fi before connecting

Information shared through public Wi-Fi hotspots in cafés, airports and hotels and other public places can be intercepted.

- Turn off automatic connection to public Wi-Fi on your devices.
- Choose to connect to non-public Wi-Fi for a more secure connection.
- Consider using a reputable Virtual Private Network (VPN) application on your device.

Australian Cyber Security Centre Contact Info

cyber.gov.au | asd.assist@defence.gov.au | 1300 CYBER1 (1300 292 371) | @cybergovau | @StaySmartOnline

ACSC Australian Cyber Security Centre

Get started now

Follow the checklist to protect yourself from scammers, cybercrime and identity theft.

Day One

2 min each

I created a strong, unique password and turned on two-factor authentication for my:

- [ ] Online bank and purchasing accounts
- [ ] Apple ID
- [ ] Google account

* which includes Gmail and YouTube

- [ ] Email accounts

* Hotmail, Yahoo, etc.

Day Two

2 min each

I created a strong, unique password and turned on two-factor authentication for my:

- [ ] Facebook
- [ ] Twitter
- [ ] Instagram
- [ ] LinkedIn
- [ ] WhatsApp

* or other messenger application

Day Three

2 min each

I added a PIN /password and turned on automatic software updates for my:

- [ ] Mobile phone
- [ ] Tablet / iPad
- [ ] Home computer
- [ ] Laptop

Day Four

30 min each

I installed security software on my:

- [ ] Mobile phone
- [ ] Tablet / iPad
- [ ] Home computer
- [ ] Laptop

Day Five

3 min each

I completed the security check-up for my:

- [ ] Gmail
- [ ] Facebook
- [ ] LinkedIn
- [ ] Laptop

Day Six

1 min each

I only connected to trusted Wi-Fi networks on my:

- [ ] Mobile phone
- [ ] Tablet / iPad
- [ ] Home computer
- [ ] Laptop

Australian Cyber Security Centre Contact Info

cyber.gov.au | asd.assist@defence.gov.au | 1300 CYBER1 (1300 292 371) | @cybergovau | @StaySmartOnline