Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre


# Secure your social media

Content Complexity
**SIMPLE** ●○○

cyber.gov.au

# For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

***Personal cyber security*** series



# Table of contents

# Secure your social media

Social media is a great way to stay in touch with friends and family, post your photos, and keep up to date with news. It is also an ideal place for cybercriminals to steal your information.

To protect yourself, secure your accounts and your information.

# Understand the threats

There can be many threats to your security and privacy when using social media. It's important to understand these threats so you can identify and avoid them in the future.

## Theft of personal information

Your personal information may be visible to more people than you would like. Cybercriminals can use the information you post to social media to commit cybercrimes. This may include identity theft, fraud or extortion. You should review your privacy settings and control who can see your information.

Social media and messaging apps can collect your information as part of their business model. They will include this in their terms of service. These terms of service can change at any time. This means the type of information they collect and how they use it can change without your knowledge.

## Malware

Cybercriminals use malware (short for 'malicious software') to gain access to your information. You might open a link or attachment that downloads malware without you knowing. Some malware may even pose as antivirus or security products. To learn more, visit cyber.gov.au/malware

## Phishing

Phishing is when someone tricks you into giving them your information by using fake emails or text messages. For example, they will pretend to be a friend, colleague, bank or government department. They may ask you to open a malicious link or attachment to steal your account details or credit card number.

Cybercriminals will use details from information you post online to seem more genuine. To learn more, visit cyber.gov.au/phishing

# Secure your accounts

Your social media accounts contain a lot of information about you. Learn about these important steps to keep your accounts secure.

## Turn on multi-factor authentication

Use multi-factor authentication (MFA) where possible. MFA is one of the best ways to add extra security to your social media accounts. MFA is when you need 2 or more steps to verify your identity before you can log in. For example, using your login details as well as an authentication code. This makes it difficult for cybercriminals to gain access to your account if they know your login details.

To find out how to turn on MFA, search 'multi-factor authentication' or 'two-factor authentication' for the social media platforms you use.

It is also crucial to turn on MFA for any email address linked to your social media accounts. If a cybercriminal gets access to your email account(s), they can lock you out of your social media accounts. To learn more, visit cyber.gov.au/mfa

## Use a strong password

Where MFA is not possible, use a strong and unique password, such as a passphrase. A passphrase has 4 or more random words like 'crystal onion clay pretzel'. Passphrases are easy to remember but hard for someone to guess.

Avoid using obvious or public details about yourself in your passphrases. For example, if you post a photo of your pet and mention its name, don't use your pet's name in your passphrases. Cybercriminals can guess them from the information you post.

Use a different passphrase for each social media account and don't share them with anyone. This includes the answers to your security questions if you need to recover your account. You can use a reputable password manager to create and store unique passphrases.

To learn more, visit cyber.gov.au/passphrases

# Protect your privacy

Not everyone has your best interests in mind and may use what you share online to their advantage. Familiarise yourself with these important steps when using social media or messaging apps.

## Practice secure social media habits

Lock your device whenever you leave it unattended, even if it is only for a short period. Also set your devices to automatically lock after a short time (less than 5 minutes). That way if someone has taken your device, they won't be able to access your social media and messaging apps.

Be careful when allowing third-party apps to access your social media accounts. This can create another way for cybercriminals to gain access. You should review and remove any third-party apps you don't need or recognise.

Never save your login details on a shared public device and always sign out when you finish. Otherwise, anyone could log in and use your account, such as from a travel lounge, library or school computer.

Don't connect to unsecure public Wi-Fi to access your social media or messaging apps. It may seem enticing to use free public Wi-Fi, but anyone can set up a hotspot and steal your information. Always try to use a trusted network such as your home Wi-Fi or mobile data. Where this is not an option, think twice about what you share or access on unsecure public Wi-Fi. To learn more, search 'connecting to public Wi-Fi and hotspots' on cyber.gov.au

Avoid opening social media links someone has sent you. Cybercriminals may pretend to be someone you know to steal your login details or install malware on your device. Even your friends and family could be sharing malicious links without realising. If in doubt, log in through the official website or app and make sure the URL starts with 'https' ('s' stands for secure).


**Case study: The Instagram hacker**

Becky from Victoria received a message on Instagram from a friend with a link in it. The link didn't seem suspicious so she opened it, but it led to a blank page. Five minutes later, Becky was signed out of her Instagram account and could not log back in. It turned out a cybercriminal had sent the link and now had control of Becky's account.

The cybercriminal then sent a message to Becky's friends about a bitcoin scam, which included a malicious link. Becky made a new account to talk to the cybercriminal to try and get her account back. But, the cybercriminal blocked all contact with Becky.

This case study shows why it is important to stay vigilant and practice secure habits.

## Review your privacy settings

Make sure to review your default privacy settings to control who can see your information. This will help stop cybercriminals from learning more about you. Check your privacy settings often and review any updates to terms of service that may affect it.

The eSafety Commissioner has detailed information on social media and messaging platforms. To learn more, visit esafety.gov.au/esafety-guide

## Limit the information you post

Once you post something online, it is out there for anyone to see and can be very difficult to remove. Be careful of sharing information such as your:

- phone number
- email address
- home address
- date of birth
- bank and credit card details
- employment details
- school or university (including where your children go for school or childcare).

Be aware of what your photos can reveal about you. Avoid including location details such as check-ins, street signs and metadata. You can go one step further by changing your settings so your friends and family can't tag you in their photos.

## Delete your unused accounts

Get rid of any social media and messaging accounts you no longer use. Leaving them active can expose your information if you're not checking them.

Remember that uninstalling an app doesn't delete or deactivate your account. You will need to do this through the official app or website.

# Protect yourself from scams

Cybercriminals will often pretend to be someone you know or trust. Learn about the warning signs of a compromised social media account or phishing attempt.

## Identify fake and compromised accounts

Cybercriminals can set up fake accounts or hack real ones to learn more about you, often posing as a brand or influential person. Their goal is to get you to reveal information to steal your identity or money. Be wary of contact and friend requests from people you don't know.

Warning signs of a fake account include:

- a low number of friends or followers
- very little activity or a recent activation date
- few photos, low-quality photos or stock photos.

Inspect what they post and share online. If it appears generic, or like spam, it could mean the profile is fake. You can also do a reverse image search to check if their photos appear on other profiles.

Cybercriminals can also impersonate your friends and family. If in doubt, check with the person you know in another way, such as on a call or in person.

You should block and report fake accounts through your social media platform. To learn more, search 'report' for the social media platforms you use.

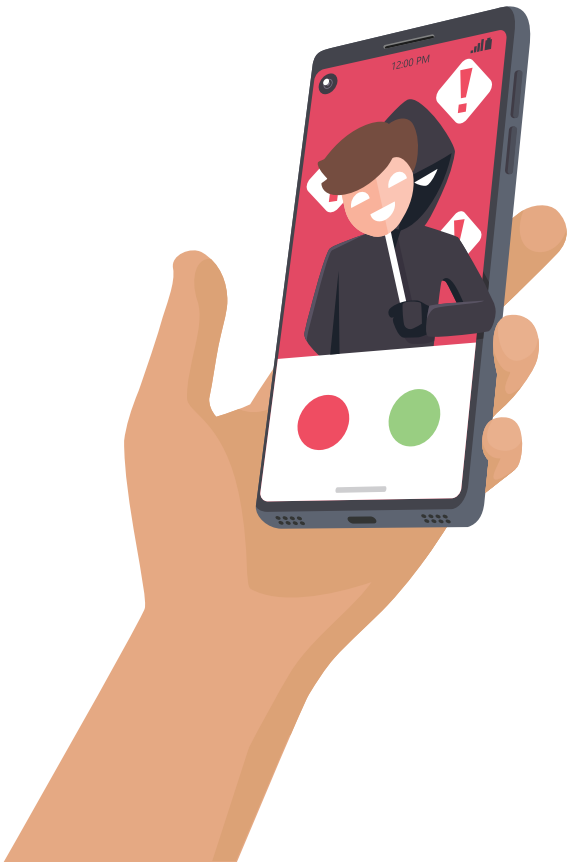
For more advice on other social media and messaging apps, visit esafety.gov.au/esafety-guide

## Be wary of online shopping scams

Cybercriminals can create a fake business page on social media, even copying their posts or reviews to appear more credible. Always check for slight variations in the business name or social media handle.

When buying products through social media, such as an online shop or marketplace, check the seller's profile first. Be wary of sellers that have a new profile, a private page or little to no customer engagement. Also look out for cheap products or deals that seem too good to be true. If it seems like a scam, it probably is.

To learn more, search 'online shopping' on cyber.gov.au



# More resources

## Report and recover

If you think a cybercriminal has compromised your social media account, visit cyber.gov.au/report-and-recover
You can find out what to do to protect yourself from further harm.

## eSafety Commissioner

The eSafety Commissioner helps safeguard all Australians from online harm. They promote safe and positive online experiences. Topics include the risks of online chat, including advice for women and young people. To learn more, visit esafety.gov.au

## Scamwatch

Scamwatch is run by the National Anti-Scam Centre. They collect reports about scams to help warn others and stop scams. They also have the latest advice on how to spot and avoid scams, such as social media scams. To learn more, visit scamwatch.gov.au

## Social media advice for organisations

If you need advice for your business, search 'security tips for social media and messaging apps' on cyber.gov.au

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.



**For more information, or to report a cyber security incident, contact us:**
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre