Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Security tips for social media and messaging services

First published: August 2011
Last updated: April 2026

Introduction

Social media and messaging services can pose risks to the security and privacy of individuals and the organisations they work for. This guidance provides an overview of those risks along with recommendations for organisations and their staff in order to assist in securing social media and messaging accounts as well as their mobile apps.

Risks of using social media and messaging services

Exploitation of personal information

Personal information posted to social media, or shared via messaging apps, can be exploited. Even seemingly benign posts, messages, photos or videos can be used to develop detailed profiles of individuals. This information could be used in social engineering or espionage campaigns aimed at obtaining sensitive information, or influencing individuals to compromise their organisation's activities or systems.

Data collection

Social media and messaging services (e.g. Facebook, Instagram, LinkedIn, Messenger, Pinterest, Reddit, Signal, Snapchat, Telegram, TikTok, Twitter, WeChat, WhatsApp, YouTube and others) typically collect extensive data as part of their business model. These services may also collect additional data from individuals' devices, which extends beyond the content of messages, videos and voice recordings. Note, the type of data collected may change over time, including when new versions or features are released. The terms of use and privacy policies relating to what data is collected, as well as how and when it can be used, may also change at short notice or be difficult to understand. Sometimes this data is stored outside of Australia and may be subject to lawful access or covert collection by other countries. In such cases, current Australian legislation and privacy or consumer laws may not apply.

Identity theft, fraud, reputation damage and embarrassment

Due to their popularity, social media and messaging services are also a common way for malicious actors to gather information on individuals as well as their organisation's activities and systems. When personal or sensitive information is posted to social media, or shared via messaging apps, this has the potential to cause reputational damage or embarrassment for individuals and organisations. Information that appears to be benign in isolation could, if aggregated with other information, breach individuals' privacy or organisational security.

Recommendations for organisational use

Organisations should take into account vendor transparency and their commitment to the security of their products and services when selecting which social media and messaging services to use.

The following measures should be implemented for the use of organisational social media and messaging accounts:

- Ensure only authorised staff have access to organisational social media and messaging accounts, and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for access.
- Ensure staff are informed of, and agree to, their organisation's social media and messaging usage policies.
- Ensure staff are trained on the use of organisational social media and messaging accounts.
- Ensure staff are aware of what can and cannot be posted to social media, or shared via messaging apps, using organisational social media and messaging accounts.
- Ensure staff are aware of processes for responding to the posting of sensitive or inappropriate information to social media, or shared via messaging apps.
- Ensure staff are aware of processes for regaining control of hijacked organisational social media and messaging accounts.

Recommendations for staff use

The use of social media and messaging services by staff should be governed by common sense and a healthy level of scepticism. For example, there have been numerous incidents where social media has been used to distribute inaccurate information (i.e. 'fake news'). Furthermore, other incidents have involved accurate information being redistributed by a very large number of automated accounts (i.e. 'bots') in an effort to draw additional attention or to sway reader opinion. Finally, other incidents have involved malicious actors masquerading as support staff in order to attempt covert social media and messaging account access for espionage purposes.

The following measures should be implemented for the use of personal social media and messaging accounts by staff:

- When creating personal social media or messaging accounts, use an alias rather than disclosing your full name.
- Use a personal email address rather than an organisational email address. If possible, use a separate personal email address for social media and messaging services.
- Ensure privacy options for social media and messaging accounts are understood and applied. For example, use private profiles and disappearing messages where appropriate.
- Avoid mixing organisational and personal information via social media and messaging accounts.
- Carefully consider the type of information posted to social media, or shared via messaging apps, as it can be very difficult to remove or recall what was previously posted or shared.
- Maintain situational awareness of group membership for social media and messaging accounts. Remove accounts that do not have a legitimate requirement for group membership.

- Restrict the amount of personal information posted to social media, such as home or work addresses, phone numbers, place of employment, and any other sensitive information, such as security clearances or job skills.
- Within reason, monitor information posted about you on social media by others to prevent disclosure of your personal information.
- If locations or movements are sensitive, be aware of social media and messaging services that automatically post such information.
- Remove location data from any pictures before posting to social media, or sharing via messaging apps.
- Be wary of accessing shared links or attachments, including via social media and messaging services.
- Be wary of unsolicited contact via social media and messaging services. Avoid accepting requests from unknown people.

Securing social media and messaging accounts

The following measures should be implemented for securing the use of both organisational and personal social media and messaging accounts:

- Where possible, use multi-factor authentication to protect access to social media and messaging accounts accessed via web browsers. Otherwise, use a unique password for each social media and messaging account.
- Do not share passwords, registration codes or verification codes for social media and messaging accounts, especially with other accounts claiming to belong to vendor support staff.
- Do not elect to remember passwords for social media and messaging accounts, unless stored in a password vault.
- If asked to set up security questions to recover social media and messaging accounts, do not provide answers that could easily be obtained from public sources of information.
- Do not use social media and messaging accounts from untrusted devices, such as in internet cafes or hotels.
- Do not configure social media and messaging accounts to automatically sign in on shared devices.
- Always remember to sign out of social media and messaging accounts after use on shared devices.
- Use lock screens and a password on any devices that have access to social media and messaging accounts.
- Remember to close old social media and messaging accounts when they are no longer required.

Securing the use of social media and messaging apps

Most social media and messaging vendors provide a mobile app for use on the go. These social media and messaging apps can create additional security and privacy risks that should be considered before their installation. The following measures should be implemented for the use of social media and messaging apps:

- Where possible, use biometric authentication to protect access to social media and messaging accounts accessed via social media and messaging apps.
- Ensure devices use the latest available operating system in order to control individual social media and messaging app permissions.
- Only install social media and messaging apps from trusted stores, such as the Google Play Store or the Apple App Store.
- Be wary of social media and messaging apps that require or request excessive permissions for the functions they provide.
- Make sure to check for, and update, social media and messaging apps on a regular basis.
- Make sure to check social media and messaging app permissions and security settings after updates, as these can change over time.

Further information

The *Information security manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to mitigate cyber security incidents*, along with its Essential Eight, complements this framework.

Further information on detecting socially engineered messages is available in the *Detecting socially engineered messages* publication.

Further information on enabling multi-factor authentication for social media accounts is available in the *Protect Yourself: Multi-factor authentication* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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