Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Security Tips for Social Media and Messaging Apps

First published: August 2011
Last updated: July 2022

Introduction

Social media and messaging apps can pose risks to the security and privacy of individuals and organisations. This guidance provides an overview of those risks along with recommendations for business and personal use in order to assist in securing social media accounts as well as social media and messaging apps.

Risks of using social media and messaging apps

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 extortion or social engineering campaigns aimed at eliciting sensitive information, or influencing individuals to compromise organisations' activities or systems. In addition, social media content may not come from reputable or trustworthy sources and may contain disinformation.

Data collection

Social media and messaging apps (e.g. Facebook, Instagram, LinkedIn, Messenger, Pinterest, Reddit, Snapchat, Telegram, TikTok, Twitter, WeChat, WhatsApp, YouTube and others) typically collect extensive data as part of their business model. These apps 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 apps are also a common way for malicious actors to gather information on individuals as well as organisations' activities and systems. Even social media and messaging apps targeted at children or teenagers present a risk that personal or sensitive information may be collected. 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. Information that appears to be benign in isolation could, if aggregated with other information, breach users' privacy.

Recommendations for business use

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

The following measures should be implemented for the use of corporate social media accounts:

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

Recommendations for personal use

The use of social media for personal purposes 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.

The following measures should be implemented for the use of personal social media accounts:

- When creating social media accounts, use an alias rather than disclosing full names.
- Use a personal email address rather than a business email address. If possible, use a separate personal email address for social media.
- Ensure privacy options are understood and applied. Use a private profile where appropriate.
- 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.
- Within reason, monitor information posted about you by others to prevent disclosure of personal information.
- If locations or movements are sensitive, be aware of social media and messaging apps that automatically post such information.
- Remove location data from any pictures before posting to social media or sharing via messaging apps.
- Carefully consider the type of information posted to social media, or sent via messaging apps, as it can be very difficult to remove or recall what was previously posted or sent.

- Be wary of accessing shared links or attachments, including via social media and messaging apps.
- Be wary of unsolicited contact. Avoid accepting requests from unknown people.

Securing the use of social media accounts

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

- Where possible, use multi-factor authentication. Otherwise, use a unique passphrase for each social media account.
- Do not share or email passphrases for social media accounts.
- Do not elect to remember passphrases for social media accounts, unless stored in a password vault.
- If asked to set up security questions to recover social media accounts, do not provide answers that could easily be obtained from public sources of information.
- Do not use social media accounts from untrusted devices, such as in internet cafes or hotels.
- Do not configure social media accounts to automatically sign in on shared devices.
- Always remember to sign out of social media accounts after use on shared devices.
- Use lock screens and a passphrase on any devices that have access to social media accounts.
- Remember to close old social media accounts when they are no longer required.

Securing the use of mobile apps

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

- Ensure devices use the latest available operating system in order to control individual mobile app permissions.
- Only install mobile apps from trusted stores, such as the Google Play Store or the Apple App Store.
- Be wary of mobile apps which require or request excessive permissions for the functions they provide.
- Make sure to check for, and update, mobile apps on a regular basis.
- Make sure to check mobile 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 common types of scams is available from the Australian Signals Directorate.

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