Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Security Tips for Social Media and Social Networking Apps

JULY 2020

Introduction

Social media, and social networking or messaging apps, can pose a number of security and privacy risks to both organisations and individuals when used in an inappropriate or unsafe manner.

Due to their popularity, social networking or messaging apps are a common way for an adversary to gather information on organisations and their employees, projects and systems. Even social networking or messaging apps targeted at children or teenagers present the risk that sensitive or embarrassing information will be disclosed. When sensitive or embarrassing information is posted on social networking platforms, or shared via messaging apps, it has the potential to harm individuals and Australia's national interests, security or economic wellbeing. Information that appears to be benign in isolation could, if aggregated with other information, have a considerable impact.

Personal information posted on social networking platforms, or shared via messaging apps, can also be used by an adversary. Even seemingly benign posts, messages, photos or videos can be used to develop a detailed profile of an individual's lifestyle and hobbies. This information could be used in extortion or social engineering campaigns aimed at eliciting sensitive information from or influencing individuals to compromise an organisation's systems.

Information which is posted to social networking platforms (even in private or direct messages), or through social networking or messaging apps, may be accessible to social networking and mobile app companies. Sometimes, this information can be stored outside of Australia and subject to lawful and covert data collection requests by other countries, and you may not be protected by Australian legislation and privacy or consumer laws.

The compromise of social networking accounts could also contribute to identify theft, fraud and/or reputation damage or embarrassment to individuals.

Social networking for business purposes

The use of social networking platforms for business purposes should be governed by organisations' social media usage policies.

The following measures should be implemented for corporate social networking accounts:

- Ensure only authorised users have access to corporate social networking accounts.
- Be aware of any extrajudicial obligations in conflict with Australian law which may apply to social networking or mobile app companies.
- Ensure users are informed of, and agree to, their organisation's social media usage policies as well as social network platforms' usage policies.
- Ensure users are trained on the use of corporate social networking accounts.

- Ensure users are aware of what can and cannot be posted using corporate social networking accounts.
- Ensure users are aware of processes for responding to posting of sensitive or inappropriate information.
- Ensure users are aware of processes for regaining control of hijacked corporate social networking accounts.
- Ensure users' access to corporate social networking accounts (either direct or delegated) is revoked immediately when there is no longer a requirement for access.

Social networking for personal purposes

The use of social networking platforms for personal purposes should be governed by common sense and a healthy level of scepticism. For example, there have been numerous incidents where social networking platforms have 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 in an effort to draw additional attention or to sway reader opinion.

The following measures should be adopted by individuals for the use of their personal social networking accounts:

- When creating social networking accounts use an alias rather than disclosing your full name.
- Use a personal email address rather than a business email address. If possible, use a separate personal email address for social networking.
- Ensure you understand and apply any available privacy options and use a private profile where available. All the information you put on social networking, or share on social networking apps will be available to the app or social networking company regardless of privacy settings.
- Restrict the amount of personal information placed on social networking such as your home or work address, phone numbers, place of employment, and any other personal information that can be used to target you.
- If your location or movements are sensitive, be aware of mobile social networking apps that automatically post your location. Also, remove GPS coordinates from any pictures posted.
- Do not post information that is not for public release from your current or previous jobs.
- Carefully consider the type and amount of information you post. Remember the internet is permanent and you can never fully remove what has been posted. Further, all your posts will be available to the social networking platform's operators regardless of your privacy settings.
- Monitor information friends post about you to prevent the unauthorised disclosure of your personal information.
- Be wary of accessing shared links or attachments including via 'direct' or 'private' messages on social networking platforms and messaging apps.
- Be wary of unsolicited contacts. Do not accept requests from people that you do not know.

Securing social networking accounts

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

- Use a strong passphrase that is unique for each social networking account and is not re-used on any other system. Use multi-factor authentication where possible.
- Do not share passphrases for social networking accounts.
- Do not store passphrases for social networking accounts in emails or in documents.
- Do not elect to remember passphrases for social networking accounts when offered by web browsers.

- Avoid configuring social networking accounts to automatically sign in.
- Always remember to sign out of social networking accounts after use.
- If asked to set up security questions to recover social networking accounts, do not provide answers that could easily be obtained from public sources of information.
- Do not access social networking accounts from untrusted devices in internet cafes or hotels.
- Use lock screens and a passpassphrase on devices that have access to social networking accounts.
- Where possible, access social networking accounts using devices that are using the latest versions of software and have had all recent updates applied.
- Remember to close old social networking accounts when they are no longer required.

Securing mobile app permissions

Most social networking platforms provide a mobile app for use on the go. These mobile apps can create additional security and privacy risks which should be considered before installation, and be reviewed regularly:

- Ensure you are informed of, and agree to, social networking platforms' usage policies which may include collection of data about you and your device.
- Ensure your device is up-to-date with the latest available operating system which provides the greatest control of mobile app security settings.
- Only install mobile apps from your device's approved app store, such as Google Play or the Apple App Store.
- Check the mobile app's store page for required permission before you install any mobile app. Be wary of mobile apps which require excessive permissions for the functions they provide.
- Also make sure to check mobile app permissions and security settings after updates as these can change over time.
- Be mindful that mobile app permissions and privacy settings cannot completely remove the risk of your information being compromised. Sometimes mobile apps can collect more information about you and your device than they openly declare. It is important that you trust the social networking platform you are using with your information and access to your device.
- Be aware that information collected and transmitted offshore may not attract protection through Australian legislation and privacy or consumer laws.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

For more information on detecting socially engineered messages, see the ***Detecting Socially Engineered Messages*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/detecting-socially-engineered-messages.

For more information on securing personal devices, see the ***Security Tips for Personal Devices*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/security-tips-personal-devices.

For more information on enabling multi-factor authentication for social media accounts, see the following publications:

- ***Turning on Two-Factor Authentication – Apple ID*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-apple-id
- ***Turning on Two-Factor Authentication – Facebook*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-facebook
- ***Turning on Two-Factor Authentication – Gmail*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-gmail
- ***Turning on Two-Factor Authentication – LinkedIn*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-linkedin
- ***Turning on Two-Factor Authentication – Microsoft Accounts*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-microsoft-accounts
- ***Turning on Two-Factor Authentication – Twitter*** at https://www.cyber.gov.au/acsc/view-all-content/guidance/turning-on-two-factor-authentication-twitter.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.