Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Security Tips for Social Media

JANUARY 2019

Introduction

Social media can pose a number of risks to both organisations and individuals when used in an inappropriate or unsafe manner.

Due to its popularity, social media is a common way for an adversary to gather information on organisations and its employees, projects and systems. When sensitive or inappropriate information is posted on social media, it has the potential to harm Australia's national interests, security or economic wellbeing. Information that appears to be benign in isolation could, if collated with other information, have a considerable impact.

Personal information posted on social media can also be used by an adversary. In particular, it can be used to develop a detailed profile of an individual's lifestyle and hobbies. This information could be used in social engineering campaigns aimed at eliciting sensitive information from individuals or influencing individuals to compromise an organisation's systems.

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

Social media for business purposes

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

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

- Ensure only authorised users have access to corporate social media accounts.
- Ensure users are informed of, and agree to, 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 using corporate social media 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 media accounts.
- Ensure users' access to corporate social media accounts (either direct or delegated) is revoked immediately as soon as there is no longer a requirement for access.

Social media for personal purposes

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 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 media accounts:

- When creating social media 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 media.
- Apply any available privacy options and use a private profile where available.
- Restrict the amount of personal information placed on social media 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 social media 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.
- 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 messaging services.
- Be wary of unsolicited contacts. Do not accept requests from people that you do not know.

Securing social media accounts

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

- Use a strong password that is unique for each social media account and is not re-used on any other system. Use multi-factor authentication where possible.
- Do not share passwords for social media accounts.
- Do not store passwords for social media accounts in emails or in documents.
- Do not elect to remember passwords for social media accounts when offered by web browsers. Avoid configuring social media apps to automatically sign in.
- 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 access social media accounts from untrusted devices in internet cafes or hotels.
- Always remember to sign out of social media accounts after use.
- Use lock screens and a password on devices that have access to social media accounts.
- Where possible, access social media accounts using devices that are using the latest versions of software and have had all recent updates applied.
- Remember to close old social media accounts when they are no longer required.

Further information

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

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

For more information on detecting socially engineered messages sent via social media, see the ***Detecting Socially Engineered Messages*** publication at https://www.acsc.gov.au/publications/protect/Socially_Engineered_Messages.pdf.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).