18 April 2023/CRA-2023-1000

Cyber Resilience Advice

National Cyber Security Centre

*The Traffic Light Protocol (TLP) marking is used to ensure that sensitive information is shared with the correct audience. Recipients can spread **TLP: CLEAR** information to the world, there is no limit on disclosure. Information sources may use **TLP: CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP: CLEAR** information may be shared without restriction.*

Assessing the risks of social media applications on government mobile devices

This cyber security advisory sets out considerations to assist New Zealand Government agencies in making risk-based decisions about the use of social media applications (apps) on government phones and other devices.

This guidance will:

a) help you to understand the technical and national security risks relating to social media apps

b) help to inform your risk assessment process for approving social media apps.

// Who is this advice for?

This resilience advice is designed to help agencies to make informed risk decisions about using social media apps on their agency's mobile devices. This advice will help agencies' security and risk staff to understand, assess and (where necessary) approve social media apps for use in their agency.

This advice is informed by the NCSC's understanding of the technical and national security threats that social media apps can present.

If you are a public servant and you want to use a social media app on an agency-issued mobile device, we recommend discussing this with your agency's Chief Information Security Officer or Information Technology Security Manager.

// Scope of this advice

This advice relates to social media apps installed on mobile devices that hold agency information. It is not intended to cover, and does not address, the use of social media in web browsers on laptops and desktop computers.

This paper sets out advice and considerations regarding:

a) the risks presented by downloading social media apps onto an agency device

b) how the use of social media on a device could impact an agency's security posture.

This advice does not cover the full breadth of considerations required as part of your risk assessment or controls selection process. This document provides commentary and advice on the specific security considerations that relate to installing social media apps on an agency-managed mobile device. We note that the permissions sought by social media apps, and the risks associated with them, are also relevant to a number of other classes of mobile apps.

// Assessing technology risk

Installing a social media app on a work device is a decision to install software. Agencies should understand the associated risks, treat the risks, and accept residual risks. Figure 1 (below) sets out a simplified risk assessment and acceptance process.

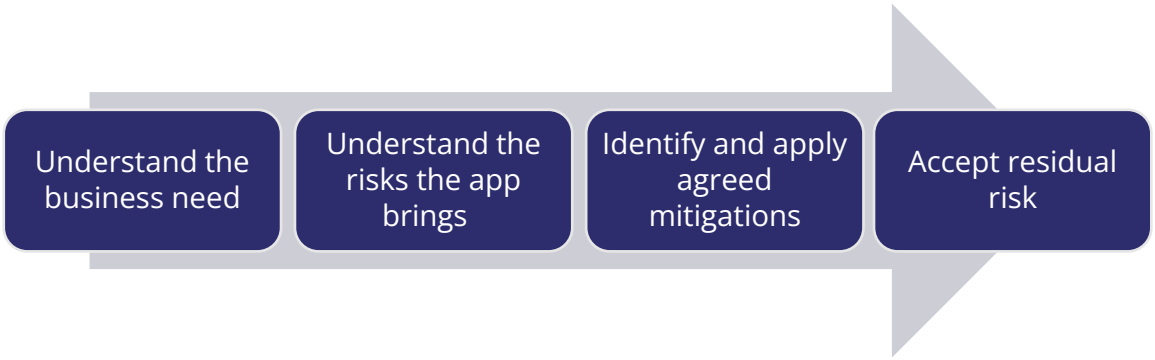

Figure 1: a high-level risk assessment process.

// What are the risks of installing social media apps?

Social media apps seek a wide range of information from a phone or mobile device to help app developers understand their audience, and these apps are often used to deliver targeted advertising to users. However, these permissions can also be used to enable a social media company to access your sensitive information, and the apps can be misused to collect information about a government agency and their staff.

The table on the next page displays a common set of permissions requested by social media apps, and how these could be misused.

How permissions are often described	Permissions that are granted	The innocent explanation	A malicious use case
Access to your camera and microphone.	Control of camera and microphone. Ability to record audio and video.	Enables the app to record videos and take photos.	Enables the app to listen to and record your activities without your knowledge.
Access to your device account (e.g. Google account or Apple ID) and device information.	Access to: • information about your device brand, model, operating system version • contact lists • mobile carrier information • wireless connection information • browsing history • keystroke patterns and rhythms.	Helps you find your friends on the platform and build your social network faster.	Uniquely identify each device across different social media platforms and websites. Uniquely identify individual users and their online behavioural patterns across different social media platforms and websites.
Access location information such as your geolocation.	Access to GPS and accelerometer information.	Showing you what's happening near you.	Track your location and build up an understanding of your movement (identifying your home, your work, and work colleagues).
Ability to read and write to storage.	Access to: • clipboard • photos • other stored media • information about other applications on the device (e.g. file names).	Your posts, associated images or videos need to be stored before they are uploaded.	Your documents, messages and files can be copied. Other apps your organisation uses can be identified.

It can be difficult to monitor or modify an app's permissions on your phone. The breadth of permissions sought by an app can help you understand the risks.

The main security risks from a social media app concern third-party access to information that is on the device(s) associated with the social media account and application.

Questions to help understand the technical threats from a social media app:

- Does your security team monitor threat and vulnerability information related to the app and device platform(s) in question?
- Does your security team validate whether the self-reported information (e.g. in privacy disclosures) provided by developers matches what is found in reality?
- What other apps and organisational information does your staff have access to from the device(s) on which social media apps would be installed?

- Do staff accounts and permissions used on their mobile devices also give them access to sensitive data sets?

Questions to help understand the potential national security threats posed by a social media app:

- How permissive is the app's privacy policy and end-user agreement? Can these agreements present a national security risk?
- Can your staff access protected or sensitive national security information from their mobile devices – for example, can they access RESTRICTED emails from the device?
- Do your staff work in sensitive locations or other places where they should not be tracked to?

// Can you reduce the scale of the risk (or avoid it)?

Risk management processes tell us that risks can be treated, avoided, transferred, or accepted. In the case of a social media app, can you avoid or reduce the scale of the risk by either prohibiting or restricting its use?

Social media applications can all have legitimate use cases to support an agency's business. But do all staff require these applications to achieve your agency's outcomes, or do only some staff need access to them?

Consider also that different mobile operating system developers and device manufacturers approach privacy controls in different ways. These controls have improved over time through operating system and security updates. This means that the types of device you provide to your staff, and how well-updated they are, will impact on the built-in options you have to manage risks.

Questions to help you understand the business need for social media apps:

- Why do staff require access to social media applications on work devices?
- Is this requirement time-limited (e.g. for campaign awareness or communicating a major policy change), or is it an ongoing part of their role (e.g. communications teams conducting social media monitoring and engagement, or regulators monitoring for banned products)?
- Could accessing social media through a web browser (rather than mobile app) meet the business needs?

// Mitigating risks

Once you have identified the risks and understand your use-case for social media, you will need to think about how you mitigate these risks.

You are unlikely to be able to modify the permissions of the app itself. Therefore, your mitigations are likely to come from restricting the organisational information or assets you install or store on the same devices as social media apps, and controlling access to that information from other apps (e.g. using containers).

The security controls you apply will be limited by the technology you use to manage your mobile devices. Mobile device management software may be able to protect your official information from being accessed. However, it is unlikely to protect against risks presented by an app's permissions to access mobile device functions such as location information or control of the camera and microphone.

Questions to help you identify potential risk mitigations:

- If some staff need access to social media platforms from a mobile device, is there additional training you can give them to help manage risks? The more you rely on policy and non-technical controls, the more important training and staff support becomes.
- Does your security policy or social media use policy provide guidance for where, when and how to use (and refrain from using) social media apps?
- Can you use dedicated devices for higher-risk apps?
- What methods do you have available to limit the amount of agency information on a device that will have social media apps on it (e.g. containers or other segregation tools)?
- Can you implement robust mobile device management to restrict social media apps' access to agency information?
- Can you implement additional protections or monitoring for devices and accounts that have social media applications?
- Do you have an ability to remotely wipe apps off devices or wipe the devices if your risk posture changes in the future?

// Summary

Downloading social media apps onto agency devices creates risks when the permissions you allow can enable external parties to access your organisation's information.

Your organisation should make carefully considered decisions about who can use social media apps, for what purpose, and how you can reduce the associated risks. Because it can be difficult to modify an app's permissions, if you want to allow social media apps on mobile devices you will need to focus on how you can control the device, and access to official information stored on it, rather than attempting to control the social media app itself.

We welcome any feedback, suggestions or constructive criticism about this advice.

The NCSC can be contacted by email at: **info@ncsc.govt.nz**

We encourage you to contact us at any time if you require any further assistance or advice.