18 April 2023

Cyber Resilience Advice

National Cyber Security Centre

Social media apps and cyber security risk: discussion points for senior leaders

Social media applications, like all software, can pose security risks. Using social media apps is different to accessing social media over the web, as the apps are downloaded onto your devices. These apps require a wide range of permissions that can be misused to monitor and record your staff, and to steal agency information including contact lists, emails and documents stored on the device.[1]

The main security risks from social media apps concern third-party access to information that is on the devices associated with the social media account and application. Some of these security risks can be controlled, depending on the technology you have available. Other risks will need to be accepted if you want to permit staff to use social media on agency devices.

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.

Your organisation should make carefully considered decisions about who can install social media apps on work devices, for what purpose, and how you can reduce the associated risks. To help you make these decisions, we recommend you talk to your **Chief Information Security Officer** (CISO).

// Questions to ask your CISO about social media app risks

a) Are our staff able to install social media apps on work phones and devices?
b) Do any of our staff have a genuine business need to use social media apps on work devices?
c) Could accessing social media through a web browser (rather than mobile app) meet the business needs?
d) What other apps and organisational information do our staff have access to on the same devices that social media apps would be installed on? Does that increase risks?
e) Does our security policy or social media use policy provide guidance for when and where to use (or refrain from using) social media apps?
f) What technical controls do we have available to reduce risks?

[1] This short advice for senior leaders is complemented by more detailed guidance from the NCSC to assist in risk assessing social media apps. You can find the guidance here:
https://www.ncsc.govt.nz/resources/information-security-guidance

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.

Te Tira Tiaki
Government Communications
Security Bureau

National Cyber
Security Centre