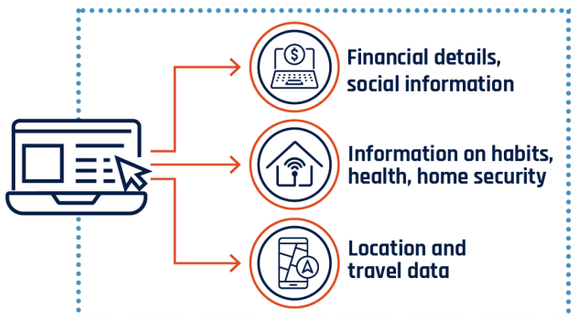
Protecting your information and data when using applications

CANADIAN CENTRE FOR CYBER SECURITY

August 2023 | ITSAP.40.200

Applications (apps) are software programs that provide the functionality to enable you to be connected, productive, creative, and entertained. You can choose from millions of apps and install them on most of the devices you and your organization rely on like cell phones, computers, tablets, and Internet of Things (IoT). Many popular apps, like Facebook, Google Drive, and Tiktok, are used by individuals and organizations for social connection, marketing, and recruitment. Given that apps are widely available and often offer free trials, it can be easy to download them without considering the security risks, like what information is being collected, stored, and shared. For example, some apps such as location-based apps, aren't designed to share data, but have a data sharing feature that collects personally identifiable information (PII) about the user and their devices. This publication provides guidance on how individuals and organizations can minimize the extent of personal and corporate information they may share with apps.

What information can apps collect?



There's a great deal of information that an app can collect from users and their devices which can be associated with an individual. The United States National Institute of Standards and Technology (NIST) Special Publication 800-122 provides examples of PII as either:

- **Information** that can be used to distinguish or trace an individual's identity (e.g. name, biometric records, and social insurance number).
- **Information** about an individual that is linked or linkable to their identity (e.g. home address, medical, financial, education, and employment information).

Be aware of metadata that you may be sharing

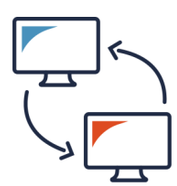
Apps can also collect **metadata** from electronic files, images, audio, video, and web pages. This is embedded information that describes the content and context of the data. Examples of metadata includes geolocation and facial recognition for image files; IP addresses, header, or packet information, and data collected in cookies for email messages.

Consider removing metadata before uploading any media files to minimize sharing potential PII. There are a number of metadata removal tools (both open source and paid versions) that are available.

What are the risks of sharing data with apps?

Apps have many social and economic benefits to our society. On the other hand, there are potential privacy concerns with them as they can gather enormous amounts of linked and linkable information on the millions of users that subscribe to their services. Here are some of the main risks with apps that share data:

- **Information may be collected without user knowledge**. User movements, behaviours, or preferences may be tracked and recorded even when the app is not in use or settings are turned off. This is a huge concern as aggregate data can reveal patterns or behaviours about individuals and organizations, or state secrets from government institutions. Aggregate data are valuable to third parties such as data brokers and advertisers who sell the information, but also to threat actors who can misuse the information for their cyber attacks.
- **Information may potentially flow across the border**. Some or all of the data may be transmitted through multiple jurisdictions or stored on a server physically located in a foreign country. If so, data may be subject to the laws of that jurisdiction that could give lawful access to your data.
- **Information may be transmitted in an unsecured manner**. Data in transit or at rest may not be encrypted and is at risk of eavesdropping and tampering.
- **Information may be shared or sold to third parties.** Many free apps or online services leverages the data they collect from their user base to sell to third parties. Advertisers and other third parties can use the information to develop targeted advertisements or communications that they sell to companies for marketing campaigns.
- **Information that is anonymized could be re-identified.** Anonymization is the process of removing or modifying PII in collected data so it can no longer be linked to an individual. Anonymization can be challenging to achieve completely as there may be remaining data elements that can be used to re-create the original data, or cross referenced with other data sources and potentially re-identify an individual.



Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Protecting your information and data when using applications

CANADIAN CENTRE FOR CYBER SECURITY

August 2023 | ITSAP.40.200

How to protect your privacy when using apps

Apps require certain settings or configurations to be enabled to ensure proper functionality. For example, a photo editing app will require access to your device's photo album and camera to function as intended. On the other hand, it may not be necessary for the same app to access your device's model name, serial number, or carrier information. It's important to know the privacy settings on the apps that you use or download. Consider the following security actions that you can take right away to protect your privacy when using apps that share data on your personal or corporately issued devices.

For organizations

- ☐ **Review the app's system-level access.** Enable permissions to essential business cases as required. For example, enable the app's access to the device's camera to obtain geolocation information only if this supports a business use.
- ☐ **Block access of unapproved apps.** Prevent users from installing unapproved apps on corporate devices. Use a monitoring tool to track attempts to download unapproved apps on your network.
- ☐ **Protect access to approved apps**. Limit the use of approved apps to only those users who have a business need. Implement multi-factor authentication (MFA) to ensure only authorized users have access to the app.
- ☐ **Apply security patches and updates**. Enable automatic updates on IT equipment and patch known vulnerabilities as soon as possible. This can help prevent implanted malware from infecting your network.
- ☐ **Establish approved settings and appropriate security permissions on corporately approved apps**. Ensure that your users understand it's their responsibility to maintain privacy settings identified by your organization.
- ☐ **Conduct audits of privacy settings on approved apps**. This will verify that they are appropriately set and that they didn't revert to the default setting after an update.
- ☐ **Educate users on tricks that apps use to obtain permissions beyond what is required**. Train users how to spot phishing attacks to avoid revealing personal or corporate information.

For individuals

- ☐ **Review the app's permissions and privacy policies.** Turn off unnecessary features and access. For example, evaluate whether an app absolutely needs access to your contact list, camera, storage, location, and microphone. If the app requires too many unnecessary permissions, then consider deleting the app.
- ☐ **Avoid using social media accounts to log into apps**. App logins through social media accounts requires you to share data and could make your accounts more vulnerable to threat actors. Create a separate login by using your email address and a unique password or passphrase. For additional privacy, consider using a throwaway email address and separate emails for each app.
- ☐ **Limit location permission**. Only allow access to your device's location when using the app, if necessary for the app's functionality.
- ☐ **Keep apps up-to-date.** Install software updates as soon as they are released so that your device will have the latest security fixes. Check the privacy settings after the update to ensure the settings and configurations haven't changed.
- ☐ **Use complex passwords or passphrases**. Ensure passwords are at least 12 characters in length and unique for each account. Use MFA wherever possible.
- ☐ **Delete unused apps**. This protects you from apps that may collect data even when they're not in use.
- ☐ **Consider using a Virtual Private Network (VPN)**. A VPN encrypts the data streams and make it appear you're located wherever the VPN service provider's network is. In addition, if your device has GPS, you can use simulation software to make it appear you're at a different location.

What to consider before you install an app

- Assess the business or personal need for the app. Evaluate the risk associated with access to your personal or confidential information against the value or benefit the app may offer.
- Research the app's developer or vendor for reviews and information on their security practices.
- Take time to understand the platform's privacy, data collection, and data use policies. Also, understand the vendor's terms and conditions and permissions requirements to know what data will be accessed and where it will be stored or transmitted. If you're not comfortable with how an app handles your PII information, then reconsider installing the app or signing up for its services.
- Check the app's user agreement to identify what metadata is collected and how it is handled. Assess your risk tolerance in the event that your data or metadata is lost or compromised.
- Understand what data and state (e.g. in transit, at rest, or in use) is encrypted by apps that claim to have end-to-end encryption.
- Download the app from trusted sources such as official app stores or from the manufacturer or vendor's website.
- Evaluate apps prior to installation and continuously throughout its useful life to ascertain it's still relevant. Organizations can explore mobile app device and application security solutions to assist in this effort.

Learn more

- Network security logging and monitoring (ITSAP.80.085)
- Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
- Best practices for passphrases and passwords (ITSAP.30.032)
- Strategies for protecting web application systems against credential stuffing attacks (ITSP.30.035)

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada