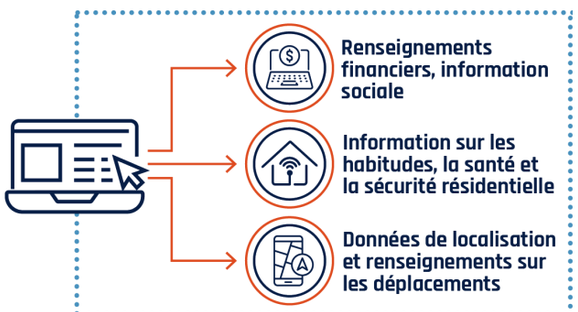
# Apprenez à protéger votre information et vos données lorsque vous utilisez des applications

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Août 2023 | ITSAP.40.200

Les applications (applis) sont des programmes logiciels qui fournissent la fonctionnalité vous permettant d'être connectée ou connecté, productive ou productif, créative ou créatif et divertie ou diverti. Il existe des millions d'applications que vous pouvez installer sur la plupart des appareils dont votre organisation et vous dépendez, comme des téléphones cellulaires, des ordinateurs, des tablettes et l'Internet des objets (IdO). De nombreuses applications populaires, notamment Facebook, Google Drive et Tiktok, sont utilisées par des personnes et des organisations pour les rapports sociaux, le marketing et le recrutement. Puisque les applis sont largement accessibles et offrent souvent des essais gratuits, il est facile de les télécharger sans considérer les risques pour la sécurité, comme l'information qui est recueillie, stockée et partagée. À titre d'exemple, certaines applications, comme les applis basées sur l'emplacement, ne sont pas conçues pour partager des données, mais comprennent une fonction de partage de données qui recueille de l'information nominative sur l'utilisatrice ou l'utilisateur et les appareils dont ils se servent. La présente publication offre des conseils visant à réduire au minimum l'étendue de l'information personnelle et organisationnelle que les personnes et les organisations peuvent partager avec les applis

## Quelle information les applications peuvent-elles recueillir?




Une application peut recueillir toute sorte d'information des utilisatrices et utilisateurs et de leurs appareils, et cette information peut ensuite servir à établir l'identité d'une personne. Dans sa publication spéciale 800-122, le National Institute of Standards and Technology (NIST) des États-Unis définit l'information nominative comme suit et en donne des exemples:

- **information** pouvant servir à déterminer l'identité d'une personne ou à remonter à une personne en particulier (p.ex.nom, données biométriques et numéro d'assurance sociale); ou
- **information** sur une personne qui est liée ou qui peut être liée à son identité (p.ex.adresse domiciliaire, renseignement médical ou financier, et information sur les études ou l'emploi).

### Attention aux métadonnées que vous pourriez partager

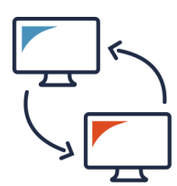
Les applications peuvent également recueillir des **métadonnées** de fichiers électroniques, d'images, de contenu audio et vidéo, et de pages Web. Les métadonnées sont des informations intégrées qui décrivent le contenu et le contexte des données. Parmi les métadonnées, on compte notamment la géolocalisation et la reconnaissance faciale pour les fichiers images; les adresses IP, l'information sur les paquets ou les en-têtes; et les données recueillies dans les témoins pour les courriels.

Envisagez de retirer les métadonnées avant de téléverser des fichiers multimédias afin de réduire le plus possible le partage potentiel d'information nominative. Il existe plusieurs outils d'extraction de métadonnées (payants et de source ouverte).

## Quels sont les risques liés au partage de données avec les applications?

Les applis présentent de nombreux avantages sociaux et économiques pour notre société. Cependant, les applications suscitent de possibles préoccupations en matière de protection des renseignements personnels puisqu'elles collectent d'énormes volumes d'information liée ou pouvant être liée aux millions d'utilisatrices et d'utilisateurs abonnés à leurs services. Voici les principaux risques liés aux applications qui partagent des données :

- **De l'information peut être recueillie à l'insu de l'utilisatrice ou de l'utilisateur**. Les déplacements, les comportements ou les préférences de l'utilisatrice ou de l'utilisateur peuvent être surveillés et enregistrés même quand l'application n'est pas utilisée ou que les paramètres sont désactivés. Ces activités soulèvent de grandes préoccupations puisque les données agrégées peuvent révéler les habitudes ou les comportements de personnes ou d'organisations, ou même des secrets nationaux d'institutions gouvernementales. Les données agrégées intéressent non seulement les tiers comme les courtières et courtiers en données et les annonceuses et annonceurs qui vendent l'information, mais également les auteures et auteurs de menace qui peuvent utiliser l'information à mauvais escient dans le cadre de cyberattaques.
- **L'information peut circuler entre les frontières**. Certaines données, voire toutes les données peuvent être transmises dans différents pays ou stockées sur un serveur situé dans un pays étranger. Dans ces cas, les données peuvent être assujetties aux lois de ces pays, qui pourraient accorder l'accès légal à vos données.
- **L'information peut être transmise de façon non sécurisée**. Les données en transit ou au repos ne sont pas toujours chiffrées et sont alors vulnérables à l'écoute clandestine et au trafiquage.
- **L'information peut être partagée avec des tiers ou vendue à des tiers**. Bon nombre d'applications et de services en ligne gratuits profitent des données qu'ils recueillent de leurs utilisatrices et utilisateurs en les vendant à des tiers. Les annonceuses et annonceurs ainsi que d'autres tiers peuvent utiliser l'information pour concevoir des annonces ou des communications ciblées qu'ils vendent à des entreprises pour des campagnes de marketing.
- **L'information anonymisée peut être désanonymisée**. L'anonymisation désigne le processus qui consiste à retirer ou à modifier l'information nominative des données recueillies afin que celles-ci ne puissent plus être liées à une personne. Ce processus peut s'avérer difficile à réaliser complètement puisque des éléments de données restants pourraient être utilisés pour recréer les données originales ou pour établir des références croisées avec d'autres sources de données et potentiellement mener à la réidentification d'une personne.



Centre de la sécurité des télécommunications
Communications Security Establishment



Canada

# Apprenez à protéger votre information et vos données lorsque vous utilisez des applications

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
Août 2023 | ITSAP.40.200

## Comment protéger vos renseignements personnels lorsque vous utilisez des applications

Afin d'assurer le bon fonctionnement des applications, certains paramètres ou certaines configurations doivent être activés. Par exemple, une appli d'édition de photos doit accéder à l'album photo et à la caméra de votre appareil pour fonctionner de façon appropriée. En revanche, cette même application n'a peut-être pas besoin d'accéder au numéro de modèle, au numéro de série ou à l'information sur l'opérateur de réseau mobile de votre appareil. Il est important de connaître les paramètres de confidentialité des applications que vous utilisez ou téléchargez. Considérez de prendre immédiatement les mesures de sécurité ci-dessous afin de protéger vos renseignements personnels lorsque vous utilisez des applications qui partagent des données sur vos appareils personnels ou organisationnels.

### Pour les organisations

- ☐ **Examiner l'accès de l'application au système**. Accordez les droits d'accès pour réaliser des activités opérationnelles essentielles, au besoin. Par exemple, accordez à l'application l'accès à la caméra de l'appareil pour obtenir l'information de géolocalisation uniquement si cette utilisation est nécessaire dans un contexte opérationnel.
- ☐ **Bloquer l'accès des applications non approuvées**. Empêchez les utilisatrices et utilisateurs d'installer des applis non approuvées sur les appareils organisationnels. Utilisez un outil de surveillance pour repérer les tentatives de téléchargement d'applications non approuvées sur votre réseau.
- ☐ **Protéger l'accès aux applications approuvées**. Limitez l'utilisation d'applications approuvées uniquement aux utilisatrices et utilisateurs qui en ont besoin dans le cadre de leurs fonctions. Mettez en œuvre l'authentification multifacteur (AMF) pour veiller à ce que seuls les utilisateurs et utilisatrices autorisés aient accès à l'application.
- ☐ **Appliquer les correctifs et les mises à jour de sécurité.** Activez les mises à jour automatiques sur l'équipement TI et corrigez les vulnérabilités connues dans les plus brefs délais. Cette mesure peut aider à empêcher les maliciels implantés d'infecter votre réseau.
- ☐ **Établir les paramètres approuvés et les autorisations de sécurité appropriées sur les applications approuvées par l'organisation**. Assurez-vous que les utilisatrices et utilisateurs comprennent qu'ils sont responsables de maintenir les paramètres de confidentialité établis par votre organisation.
- ☐ **Mener des audits des paramètres de confidentialité sur les applications approuvées.** Vous pourrez ainsi vérifier que les paramètres de confidentialités sont réglés de façon appropriée et qu'ils ne sont pas retournés aux paramètres par défaut à la suite d'une mise à jour.
- ☐ **Sensibiliser les utilisatrices et utilisateurs sur les astuces qu'utilisent les applications pour obtenir plus de droits d'accès que ceux qui sont nécessaires.** Montrez aux utilisatrices et utilisateurs à repérer les attaques par hameçonnage pour éviter de révéler de l'information personnelle ou organisationnelle.

### Pour les personnes

- ☐ **Examiner les droits d'accès et les politiques de confidentialité.** Désactivez les fonctions et les accès non requis. À titre d'exemple, évaluez si une application a réellement besoin d'accéder à votre liste de contacts, à votre caméra, à votre stockage, à votre emplacement et à votre microphone. Si l'application demande trop d'accès qui ne sont pas nécessaires, envisagez de la supprimer.
- ☐ **Éviter d'utiliser des comptes de médias sociaux pour se connecter aux applications**. En vous connectant aux applications à l'aide de comptes de médias sociaux, vous partagez des données et pourriez rendre vos comptes plus vulnérables aux auteures et auteurs de menace. Créez des justificatifs d'identité distincts en utilisant votre adresse courriel et un mot de passe ou une phrase de passe unique. Pour accroître la confidentialité, considérez d'utiliser une adresse de courriel à usage unique pour chaque application.
- ☐ **Limiter l'accès à l'emplacement.** Autorisez uniquement l'accès à l'emplacement de votre appareil lorsque vous utilisez l'application, si cette fonction est nécessaire à son bon fonctionnement.
- ☐ **Tenir à jour les applications.** Installez les mises à jour logicielles dès qu'elles sont publiées afin que les plus récents correctifs de sécurité soient appliqués à votre appareil. Vérifiez les paramètres de confidentialité après la mise à jour pour vous assurer que les paramètres et les configurations n'ont pas changé.
- ☐ **Utiliser des mots de passe ou des phrases de passe complexes**. Choisissez des mots de passe composés d'au moins douze caractères et qui sont uniques à chaque compte. Utilisez l'authentification multifacteur dans la mesure du possible.
- ☐ **Supprimer les applications qui ne sont pas utilisées**. Cette mesure vous protège des applications qui peuvent recueillir vos données même lorsque vous n'utilisez pas ces applications.
- ☐ **Envisager d'utiliser un réseau privé virtuel (RPV).** Un RPV chiffre les flux de données et affiche l'emplacement du réseau du fournisseur de services RPV au lieu de votre emplacement réel. Par ailleurs, si votre appareil a un GPS, vous pouvez utiliser un logiciel de simulation pour afficher un emplacement différent de votre emplacement réel.

## Facteurs à considérer avant d'installer une application

- Évaluez le besoin personnel ou opérationnel d'utiliser l'application. Évaluez le risque associé à l'accès à votre information personnelle ou confidentielle par rapport à la valeur ou à l'avantage qu'offre l'application.
- Faites une recherche sur le développeur ou le fournisseur de l'application pour trouver des avis et de l'information sur ses pratiques de sécurité.
- Prenez le temps de comprendre les politiques de confidentialité, de collecte de donnée et d'utilisation des données de la plateforme. Par ailleurs, assurez-vous de bien comprendre les modalités et les exigences liées aux autorisations d'accès du fournisseur afin de savoir à quelles données l'application accèdera et où elles seront stockées et transmises. Si vous n'êtes pas à l'aise avec la façon dont l'application traite votre information nominative, pensez-y deux fois avant d'installer l'application ou de vous inscrire à ses services.
- Passez en revue le contrat d'utilisation de l'application pour savoir quelles métadonnées sont recueillies et comment elles sont traitées. Évaluez votre tolérance au risque en cas de perte ou de compromission de vos données ou de vos métadonnées.
- Assurez-vous de bien comprendre quelles données, et dans quels états (p.ex. en transit, au repos ou en cours d'utilisation), sont chiffrées par l'application qui prétend offrir un chiffrement de bout en bout.
- Téléchargez l'application d'une source fiable, comme le magasin officiel de l'application ou le site Web du fabricant ou du fournisseur.
- Évaluez les applications avant de les installer et tout au long de leur vie utile pour vous assurer qu'elles sont toujours utiles. En ce qui a trait aux organisations, elles peuvent explorer les solutions de sécurité pour les applications et les appareils d'application mobile afin de les aider avec cette tâche.

### Pour en savoir plus

- Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085)
- Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)
- Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)
- Stratégies pour protéger les systèmes d'application Web contre les attaques par bourrage d'identifiants (ITSP.30.035)

Centre de la sécurité des télécommunications
Communications Security Establishment



Canada