Messagerie instantanée

Février 2024

ITSAP.00.266

Les médias sociaux et les applications de messagerie instantanée (MI) font partie de notre quotidien, tant sur le plan personnel que professionnel, et sont un moyen de communication pratique. Bien que ces applications vous permettent de communiquer plus rapidement et facilement, il faut se rappeler que leur utilisation vous rend vulnérable à diverses menaces à la sécurité. Elles sont également régies par différentes normes de sécurité établies par les nombreux développeurs d'applications.

La messagerie instantanée est-elle sécurisée?

On utilise les applications de MI au travail pour communiquer facilement et rapidement avec des collègues qui se trouvent sur les lieux de travail ou à l'extérieur du bureau. Toutefois, ces applications ne sont pas entièrement sécurisées ou confidentielles. Des auteures et auteurs de menace peuvent obtenir accès à l'information transmise. Il faut donc toujours prêter attention au niveau de sensibilité des données envoyées par l'intermédiaire de ces applications.

Certaines applications de MI sont associées à vos comptes de médias sociaux. Si vous utilisez les justificatifs d'identité de votre compte de média social pour vous connecter à une application de MI, vous établissez un lien entre ces applications. Plusieurs applications de médias sociaux et de MI appartiennent à la même société, qui peut dès lors recueillir vos données et les utiliser pour accéder aux comptes connexes. Ainsi, une ou un auteur de menace qui réussit à pirater l'un de vos comptes pourra également accéder aux données liées aux autres applications auxquelles il est connecté.

Comment les auteures et auteurs de menace exploitent-ils les applications de messagerie instantanée?

Il faut considérer les nombreux risques avant d'utiliser la MI comme moyen de communication. Par exemple, l'information que vous utilisez dans une application de MI pourrait ne pas être sécurisée, et être compromise, volée ou exposée.

Les auteures ou auteurs de menace peuvent obtenir votre information en tentant de faire ce qui suit :

- Accéder à votre environnement et aux messages chiffrés à l'aide de vos justificatifs d'identité;
- Mener des attaques par piratage psychologique et des attaques par dictionnaire au moyen de l'information personnelle recueillie à partir des comptes de médias sociaux des membres de votre personnel, et d'autres plateformes qui servent au partage d'information;
- Infecter un dispositif au moyen d'un maliciel ou d'un espiogiciel en vue de compromettre et de voler de l'information.

Même si vous faites appel aux services d'un fournisseur légitime et digne de confiance, les auteures et auteurs de menace peuvent tirer avantage de failles et de vulnérabilités inconnues dans les applications. Votre information sensible court, ce faisant, le risque de tomber entre de mauvaises mains.

Le chiffrement de bout en bout est-il sécurisé?

Le chiffrement de bout en bout est un service de protection de la confidentialité qui consiste à chiffrer les données de l'expéditeur et à convertir l'information pour en masquer le contenu. Il prévient tout accès non autorisé de manière à ce que seul la ou le destinataire puisse les déchiffrer. Plusieurs applications de MI ont recours au chiffrement de bout en bout pour sécuriser votre information et vos messages. Bien que ce service semble offrir un niveau élevé de sécurité lors de l'envoi et de la réception de l'information, il est préférable de ne pas miser uniquement sur le chiffrement de bout en bout pour protéger vos données. Les auteures et auteurs de menace peuvent compromettre vos dispositifs en vue de récupérer les données non chiffrées qu'ils contiennent et de les déchiffrer ultérieurement. Dans certaines applications de MI, le chiffrement de bout en bout ne s'applique qu'aux messages en transit, et non aux messages inactifs, comme ceux qui ont été stockés ou sauvegardés. Il est important de tenir compte de ces points avant d'envoyer un message de nature plus sensible.

SÉRIE SENSIBILISATION

No de cat. D97-1/00-266-2024F-PDF
ISBN 978-0-660-68305-8

Quelles caractéristiques devrais-je rechercher lors de la sélection d'une application?

Lorsque vous songez à utiliser une application de MI, vous devriez vous assurer que le fournisseur a mis en place une infrastructure de sécurité robuste. La chaîne d'approvisionnement de votre organisation ne peut être plus forte que son maillon le plus faible. Cette chaîne d'approvisionnement est le lien essentiel entre votre organisation et les autres entités qui vous aident à servir votre clientèle. Pour de plus amples renseignements sur l'intégrité de la chaîne d'approvisionnement, veuillez consulter consultez l'ITSAP.00.070, *Sécurité de la chaîne d'approvisionnement pour les petites et moyennes organisations*.

Pour assurer la sécurité de votre chaîne d'approvisionnement, nous vous recommandons de vous poser les questions suivantes lorsque vous sélectionnez une application :

- Où l'application de messagerie stocke-t-elle ou traite-t-elle vos données?
  - Utilisez des applications offertes par des fournisseurs qui stockent vos données au Canada. Votre information sera ainsi protégée en vertu des lois canadiennes en matière de protection de la vie privée.
- En quoi l'architecture de l'application appuie-t-elle les mesures de sécurité mises en place par le fournisseur?
  - Assurez-vous de connaître les fonctionnalités offertes par le fournisseur (p. ex. la durée de conservation des messages, des listes de contacts et des journaux de communication).
  - Assurez-vous de connaître la durée de stockage de votre information et la méthode employée par le fournisseur pour procéder à sa destruction.
- Le fournisseur a-t-il mis en place des politiques de sécurité?
  - Choisissez un fournisseur qui applique des mécanismes d'authentification robustes, comme l'authentification multifacteur.
  - Veillez à mettre en place des plans et des procédures que vous pourrez exécuter advenant la compromission de votre compte.
- Quels protocoles le fournisseur utilise-t-il pour chiffrer les messages?
  - Le chiffrement de bout en bout ne permet pas de garantir la sécurité de votre information.
  - Assurez-vous que le fournisseur emploie les méthodes de chiffrement appropriées pour protéger vos données (p. ex. en tenant compte des messages inactifs et en transit).
- Le fournisseur emploie-t-il des applications connectées ou tierces?
  - Déterminez quelles sont les applications connectées et associées à votre information.
  - Pour savoir s'il est possible de faire confiance aux services offerts par le fournisseur, déterminez quelles sont les applications et les entreprises concernées par la prestation de ces services.
  - Assurez-vous que les services sont fournis conformément aux affirmations du fournisseur, ni plus ni moins (p. ex. transmission de données).

Comment puis-je utiliser la messagerie sécurisée en toute sécurité?

Malgré le fait que plusieurs applications de MI affirment pouvoir offrir une protection complète grâce au chiffrement de bout en bout, il est possible que l'information que vous envoyez ou recevez par l'intermédiaire de celles -ci soit subtilisée. Afin d'assurer la sécurité de votre information, nous vous recommandons de suivre les lignes directrices suivantes :

- Appliquez les plus récentes mises à jour à vos applications de MI et au système d'exploitation de votre dispositif (pour bénéficier des plus récents correctifs de sécurité);
- Utilisez un mot de passe distinct pour chaque application de MI;
- Utilisez l'authentification multifacteur pour vos comptes, lorsque ce type d'authentification est offert;
- Évitez de mentionner des détails susceptibles de révéler votre identité dans les profils de vos comptes (p. ex. votre nom et votre numéro de téléphone);
- N'utilisez pas la fonction « se souvenir de moi » et quittez l'application lorsque vous avez terminé;
- Songez à utiliser un gestionnaire de mots de passe;
- Évitez de partager de l'information sensible (comme des données bancaires ou un numéro d'assurance sociale);
- Assurez-vous qu'il s'agit bien d'un fournisseur ou d'une application légitime (p. ex. une fausse application de messagerie pourrait installer un maliciel sur votre dispositif);
- Utilisez des applications de messagerie s'exécutant sur des réseaux sécurisés et non sur des réseaux Wi-Fi publics;
- Évitez de connecter vos comptes de MI sur vos autres dispositifs (p. ex. service infonuagique, Internet des objets);
- Assurez-vous de pouvoir faire confiance aux personnes avec qui vous échangez des messages, puisque les destinataires pourraient, par exemple, effectuer des saisies d'écran de vos messages et les transmettre à d'autres personnes;
  - Vérifiez que les connexions bloquées sont bien déconnectées sur toutes les applications (puisque ces applications connexes pourraient ne pas bloquer les communications sur tous les comptes);
  - Validez l'identité de la personne avec qui vous échangez des messages en lui posant une question particulière ou en ayant recours à une clé chiffrée;
  - Analysez les pièces jointes avec un logiciel antimaliciel avant de les ouvrir.
- Pour déterminer si les fournisseurs sont fiables et dignes de confiance, consultez les commentaires sur l'utilisation à long terme de leurs applications.

Vous avez des questions ou vous avez besoin d'aide? Vous voulez en savoir plus sur les questions de cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.