Utilisation sûre des services bancaires en ligne

JUILLET 2022 ITSAP.00.080

Les services bancaires en ligne sont pratiques et permettent aux utilisateurs d'accéder à leurs données financières au moyen d'un appareil mobile ou d'un ordinateur. Bien que vos services bancaires en ligne comportent des contrôles de sécurité (p. ex. l'authentification et le chiffrement), vos renseignements sont quand même exposés à des risques. Les auteurs de menace peuvent trouver des façons d'accéder à vos comptes et à vos renseignements sensibles. Le présent document donne des astuces sur la façon de protéger vos renseignements financiers sensibles lors de l'utilisation de services bancaires en ligne.

À quoi servent les services bancaires en ligne?

Les services bancaires en ligne permettent de réaliser de nombreuses tâches, notamment :

- Consulter le solde et les relevés de comptes bancaires
- Payer des factures
- Déposer des chèques
- Transférer des fonds vers d'autres comptes
- Gérer les comptes
- Mettre en place des transactions automatiques

Les services offerts par une institution financière peuvent varier en fonction de la façon dont vous accédez à vos comptes en ligne (p.

Quels sont les risques?

Bien que les services bancaires en ligne soient généralement sûrs, les auteurs de menace peuvent trouver le moyen d'accéder à vos renseignements sensibles. Ils utilisent couramment des attaques par hameçonnage de même que des maliciels.

Attaques par hameçonnage

Un auteur de menace tente de vous soustraire des informations sensibles en communiquant avec vous par texto, par courriel ou par téléphone et en vous donnant l'impression que la communication provient d'une source légitime – votre banque, par exemple. Dans ce scénario, un auteur de menace prétend qu'il représente votre banque et vous informe que des activités inhabituelles ont été portées à votre compte et vous demande des renseignements sensibles, comme vos numéros de compte bancaire et de carte de crédit. Un auteur de menace peut aussi envoyer un courriel comportant un lien camouflé qui vous redirige vers un site Web frauduleux où vous devez saisir vos renseignements sensibles aux fins de « vérification ».

Maliciels

Un maliciel est un logiciel malveillant qui est conçu pour s'infiltrer dans un système informatique et qui peut aussi y causer des dommages. Si un maliciel a infecté votre appareil, il est possible qu'un auteur de menace recueille vos renseignements sensibles et obtienne l'accès à vos comptes, comme c'est le cas lorsqu'il a recours aux méthodes suivantes :

- L'envoi de messages d'hameçonnage avec pièces jointes et liens qui semblent provenir de vos services bancaires et dont l'objectif consiste à vous inciter à télécharger le maliciel sur votre appareil;
- L'utilisation de fausses applications bancaires ou de transferts d'argent pour recueillir vos justificatifs d'identité et ainsi accéder à vos renseignements sensibles.

Vous devez être à l'affût de nombreuses menaces lorsque vous utilisez des services bancaires en ligne. En apprenant à reconnaître les cybermenaces courantes, vous serez mieux à même de vous protéger. Pour de plus amples détails sur la façon d'éviter les attaques par hameçonnage ou les maliciels, veuillez consulter les documents Ne mordez pas à l'hameçon: reconnaître et prévenir les attaques par hameçonnage (ITSAP.00.101) et Protéger l'organisme contre les maliciels (ITSAP.00.057) qui sont offerts sur le site Web **cyber.gc.ca.**

SÉRIE SENSIBILISATION

No de cat. D97-1/00-080-2022F-PDF
ISBN 978-0-660-44133-7

Comment puis-je protéger mes renseignements bancaires en ligne?

Il existe des moyens de réduire les risques liés à l'utilisation de services bancaires en ligne. Consultez la liste des pratiques à adopter et à éviter en matière de cybersécurité afin de protéger votre compte bancaire, vos renseignements sensibles et votre argent contre les cybercriminels.

Pratiques à adopter

- **Lisez et comprenez les conditions générales d'utilisation énoncées par votre banque** afin de connaître vos responsabilités en tant que propriétaire du compte de même que les responsabilités de votre banque.
- **Verrouillez vos appareils au moyen d'un NIP** afin de les sécuriser en cas de perte ou de vol.
- **Utilisez une phrase de passe ou un mot de passe robuste pour protéger votre compte.** Pour de plus amples détails sur les mots de passe et les phrases de passe, consultez le document *Pratiques exemplaires de création de phrases de passe et de mots de passe (ITSAP.30.032)* sur le site Web du Centre pour la cybersécurité.
- **Utilisez une authentification multifacteur** (p. ex. une empreinte digitale et une phrase de passe) afin d'ajouter une couche de sécurité additionnelle en cas de compromission de la phrase de passe. Pour en apprendre davantage au sujet de l'authentification multifacteur, consultez le document *Sécurisez vos comptes et vos appareils avec une authentification multifacteur (ITSAP.30.030)*.
- **Installez un pare-feu et un logiciel antivirus** sur votre ordinateur pour vous protéger contre les cybermenaces, comme les logiciels malveillants. Pour en savoir plus sur la protection de votre ordinateur et de votre réseau, consultez le document *Les outils de sécurité préventive (ITSAP.00.058)*.
- **Appliquez les mises à jour et les correctifs à vos appareils et à vos logiciels** afin de remédier aux vulnérabilités et aux problèmes de sécurité. Pour de plus amples détails sur l'importance des mises à jour, consultez le document *Application des mises à jour sur les dispositifs (ITSAP.10.096)* publié sur le site Web du Centre pour la cybersécurité.
- **Utilisez le service de votre fournisseur d'accès ou un réseau Wi-Fi sécurisé** pour prévenir l'utilisation accidentelle d'un portail Wi-Fi usurpé (p. ex. des auteurs de menace se dissimulent dans un prétendu réseau Wi-Fi de café). Pour en savoir plus sur l'utilisation sûre des connexions Wi-Fi, consultez le document Utiliser le Wi-Fi sans compromettre la sécurité de votre organisation (ITSAP.80.009).
- **Accédez au site Web de votre banque ou téléchargez l'application de la banque uniquement à partir de sources légitimes** (p. ex. une application certifiée au moyen d'une source chiffrée [https] et appartenant à l'institution) afin de protéger vos données contre les auteurs de menace qui créent de faux sites Web ou de fausses applications.

Pratiques à éviter

- Ne communiquez pas (en personne ou en ligne) vos justificatifs d'identité à quiconque, pas même aux membres de votre famille.
- Ne stockez pas les justificatifs d'identité sur vos appareils (p. ex. au moyen d'un gestionnaire de mots de passe ou de l'option « Se souvenir de moi », ou encore dans le fichier de notes des appareils) pour éviter le vol des justificatifs d'identité en cas de perte ou de vol d'un appareil ou encore le vol des justificatifs par un logiciel malveillant.
- N'utilisez pas de renseignements personnels (p. ex. date de naissance, adresse ou nom d'un animal de compagnie) pour créer des phrases de passe, des mots de passe ou des réponses à des questions de sécurité. Les auteurs de menace peuvent recueillir ces données personnelles à partir de vos comptes sur les médias sociaux.
- N'utilisez pas un ordinateur public pour accéder à votre compte bancaire.
- Ne cliquez pas sur les liens et pièces jointes envoyés par courriel ou par texto sans confirmer au préalable les coordonnées de l'expéditeur.

Que faire si je suis victime de fraude?

Si vous avez été victime d'une fraude ou d'une tentative de fraude, communiquez immédiatement avec votre banque pour bloquer votre compte. Votre banque peut vous aider à gérer les risques en réinitialisant les justificatifs d'identité de votre compte.

Signalez l'incident au Centre antifraude du Canada en composant le 1 -888-495-8501 ou signalez-le en ligne à centreantifraude.ca.

Vous avez des questions ou vous avez besoin d'aide?
Consultez le site Web du Centre canadien pour la cybersécurité à **cyber.gc.ca**.