UTILISATION SÛRE DES SERVICES BANCAIRES EN LIGNE

SEPTEMBRE 2020 ITSAP.00.080

Les services bancaires en ligne sont pratiques et permettent aux utilisateurs d'accéder à leurs données financières au moyen d'un dispositif mobile ou d'un ordinateur. Même si, en principe, les services bancaires en ligne sont sûrs — notamment grâce à l'utilisation de mécanismes d'authentification et de chiffrement — des risques subsistent : un auteur de menaces pourrait trouver le moyen d'accéder aux données sensibles d'un utilisateur. Le présent document donne des astuces sur la façon de protéger l'information financière sensible tout en utilisant des services bancaires en ligne.

SERVICES BANCAIRES

Les institutions financières offrent, entre autres, les services bancaires en ligne suivants :

- Vérification du solde et des relevés de compte bancaire
- Paiement de factures
- Dépôt de chèques
- Transfert de fonds vers d'autres comptes
- Gestion des comptes
- Programmation de transactions automatiques

Les services offerts par une institution financière peuvent varier selon la façon dont on accède aux comptes en ligne (par exemple, à partir d'un appareil mobile ou d'un ordinateur de bureau).

QUELS SONT LES RISQUES?

Bien que les services bancaires en ligne soient généralement sûrs, les auteurs de menaces peuvent trouver le moyen d'accéder aux informations sensibles d'utilisateurs. Généralement, les auteurs de menaces ont recours à l'hameçonnage et aux logiciels malveillants.

ATTAQUES PAR HAMEÇONNAGE

Un auteur de menaces tente de vous soustraire des informations sensibles en communiquant avec vous par SMS, 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 menaces prétend qu'il représente votre banque et vous informe que des activités inhabituelles ont été portées à votre compte et vous demande de l'information sensible, comme vos numéros de compte bancaire et de carte de crédit. Un auteur de menaces peut aussi envoyer un courriel comportant un lien camouflé qui redirige l'utilisateur vers un site Web frauduleux où l'utilisateur doit saisir son information sensible aux fins de « vérifications ».

MALICIEL

Le 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 menaces collecte votre information sensible 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 services bancaires et dont le but est d'inciter le destinataire à télécharger le maliciel sur son appareil;
- l'utilisation de fausses applications bancaires ou de transferts d'argent pour recueillir les justificatifs d'identité et ainsi accéder aux informations sensibles de l'utilisateur.

L'utilisateur doit être à l'affût de nombreuses menaces lorsqu'il utilise des services bancaires en ligne. Mais en apprenant à reconnaître les cybermenaces courantes, il sera mieux à même de se protéger. Pour de plus amples détails sur la façon d'éviter les attaques par hameçonnage ou par maliciel, veuillez consulter le document *Ne mordez pas à l'hameçon : reconnaître et prévenir les attaques par hameçonnage* (ITSAP.00.101) de même que le document *Protéger l'organisme contre les maliciels* (ITSAP.00.057). Ces documents sont disponibles sur le site **cyber.gc.ca**.

SÉRIE SENSIBILISATION

COMMENT PUIS-JE PROTÉGER MES INFORMATIONS 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 informations 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 dispositifs au moyen d'un NIP** afin de les sécuriser et de les protéger 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, veuillez consulter le document *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032). Ce document se trouve sur notre site Web.
- **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 des cybermenaces, comme les logiciels malveillants.
- **Mettez à jour votre appareil et vos logiciels et appliquez les correctifs requis** 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) qui se trouve sur notre site Web.
- **Utilisez le service de votre fournisseur d'accès ou un réseau sans fil sécurisé** pour prévenir l'utilisation accidentelle d'un portail sans fil usurpé (par exemple, des auteurs de menaces se dissimulent dans un prétendu réseau sans fil de café).
- **Accédez au site web de votre banque ou téléchargez l'application de la banque uniquement à partir de sources légitimes** (par exemple, une application certifiée au moyen d'une source chiffrée [https] et appartenant à l'institution) afin de protéger vos données contre les auteurs de menaces 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 votre appareil (par exemple, au moyen d'un gestionnaire de mots de passe ou de l'option « Se souvenir de moi » ou encore dans le fichier de notes de l'appareil) – cela permet d'éviter le vol des justificatifs d'identité en cas de perte ou de vol de l'appareil ou encore le vol des justificatifs par un logiciel malveillant.
- N'utilisez pas des informations personnelles (par exemple, date de naissance, adresse, 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 menaces 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 message texte sans confirmer au préalable les coordonnées de l'expéditeur.

QUE FAIRE SI JE SUIS VICTIME D'UNE FRAUDE?

Si vous avez été victime d'une fraude ou d'une tentative de fraude, contactez immédiatement 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 en vous rendant au site suivant : centreantifraude.ca.

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**.