Comment faire des achats en ligne en toute sécurité

Novembre 2023

ITSAP.00.071

Il n'y a rien de plus commode que les achats en ligne : vous pouvez acheter des articles à partir de votre appareil mobile et les recevoir à domicile le lendemain. Vous devriez toutefois connaître les menaces associées à ce type d'achat, puisqu'elles présentent de nombreux risques, non seulement pour vos renseignements personnels, mais aussi pour les actifs de votre organisation, comme une adresse courriel, une adresse d'expédition, un numéro de téléphone ou un numéro de carte de crédit. En adoptant des pratiques sûres lorsque vous faites des achats en ligne pour vous ou votre entreprise, vous aiderez à assurer la confidentialité de vos actifs et renseignements sensibles. Le présent document porte sur les différentes façons de vous protéger, vous et votre organisation, lorsque vous faites des achats en ligne.

Quelles sont les menaces possibles?

En faisant des achats en ligne, vous vous exposez, tout comme votre organisation, au vol d'identité, au piratage et à des pertes financières. Voici quelques exemples des méthodes auxquelles les auteures et auteurs de menace peuvent avoir recours pour voler vos renseignements sensibles et pirater vos comptes :

- De faux sites marchands recueillent vos renseignements lorsque vous faites un achat que vous croyez réel;
- Des sites frauduleux de traitement des paiements, comme des accords financiers avec des tiers, collectent votre argent lorsque vous croyez faire une véritable transaction;
- Des sites Web non chiffrés exposent vos renseignements;
- Des sites Web non sécurisés dont les vendeurs ne sont pas nécessairement dignes de confiance, comme des vendeurs autonomes ou des particuliers.

Quels sont les signes avant-coureurs?

Vous devriez tenir compte des signes avant-coureurs suivants pour déterminer la fiabilité d'un site Web :

- Le site semble mal conçu et non professionnel;
- Les liens et le bouton Précédente sont brisés ou désactivés;
- Aucune coordonnée n'est affichée sur le site Web;
- La politique de retour ou de protection des renseignements personnels est ambiguë ou introuvable;
- On vous demande de donner les justificatifs d'identité associés à votre carte de crédit pour d'autres raisons que pour faire des achats;
- Le prix des articles est étonnamment bas ou on vous propose des aubaines qui semblent trop belles pour être vraies;
- Les frais d'expédition, les droits de douane et les frais supplémentaires semblent anormaux.

Les auteures et auteurs de menace profitent de la plus grande présence des magasins et des détaillants en ligne pour trouver de nouvelles façons de voler de l'information ou de commettre des fraudes.

SÉRIE SENSIBILISATION

No de cat. Dnn-n/nn-nnn-2022F-PDF
ISBN nnn-n-nnn-nnnnn-n

Comment puis-je me protéger?

Lorsque vous faites des achats en ligne, vous pouvez vous protéger, vous et votre organisation, en adoptant certaines pratiques, dont les suivantes :

Ces pratiques vous aideront à vous protéger lorsque vous faites des achats en ligne.

Bien qu'elles puissent réduire les risques, elles ne sauraient les éliminer entièrement.

Renseignez-vous au sujet du détaillant

- Lisez les politiques de retour et de protection des renseignements personnels des sites Web, etc.
- Lorsque vous faites des achats sur un site de réseau social comme Facebook ou Instagram, renseignez-vous au sujet de la personne ou du fournisseur pour vous assurer qu'une vérification a bien été effectuée par la plateforme et consultez les commentaires des autres acheteuses et acheteurs.

Naviguez sur le Web en toute sécurité

- Faites vos achats sur des sites Web dont l'adresse commence par HTTPS et qui ont recours à des stratégies de chiffrement pour protéger vos renseignements.
- Assurez-vous que les sites Web affichent un cadenas vert dans la barre d'adresse (un cadenas ouvert ou manquant signifie que les données du site Web ne sont pas sécurisées).
- Faites preuve de prudence lorsque vous naviguez à partir de votre téléphone mobile, car les adresses URL sont abrégées et pourraient vous amener par la ruse à visiter des sites Web malveillants.

Protégez vos comptes

- Créez une phrase de passe unique et robuste pour chacun compte en ligne (évitez d'utiliser la même phrase de passe pour plusieurs comptes).
- Ayez recours à l'authentification multifacteur (AMF).
- Vérifiez fréquemment vos relevés de carte de crédit.
- Utilisez une forme de paiement sécurisée, comme une carte de crédit délivrée par une grande institution financière qui garantit le remboursement des transactions frauduleuses.

- Lorsque le site Web ne vous est pas familier, utilisez un numéro de carte de crédit virtuel ou une carte distincte dont la limite d'achat est peu élevée (les institutions financières offrent des cartes de crédit temporaires au montant fixe que vous pouvez utiliser à la place de votre carte habituelle pour limiter les dommages).

Prenez des précautions supplémentaires

- Limitez les renseignements personnels que vous révélez sur un site Web (par exemple, ne donnez pas votre numéro d'assurance sociale).
- Concluez la transaction en tant qu'invitée ou invité pour éviter que le site Web n'enregistre vos renseignements (si vous créez un compte et enregistrez les détails de vos paiements, ayez recours à l'AMF et à une phrase de passe pour protéger vos renseignements).
- Faites des copies de sauvegarde et des mises à jour de vos appareils, et appliquez les correctifs nécessaires.
- Utilisez un réseau Wi-Fi sécurisé avec une phrase de passe robuste (utilisez des données cellulaires ou connectez-vous à un réseau virtuel privé si vous employez un réseau public).
- Faites attention aux courriels frauduleux (ne cliquez pas sur des liens contenus dans des courriels qui vous offrent des aubaines extraordinaires).

Que dois-je faire si je suis victime de fraude?

Il est parfois difficile de reconnaître les cybermenaces avant qu'il ne soit trop tard. Si vous êtes victime de fraude ou d'une compromission potentielle, vous devez prendre les mesures suivantes pour signaler et atténuer l'incident :

1. Signalez l'incident à la ou au responsable de la sécurité, à la haute direction ou au soutien technique de votre organisation;
2. Communiquez avec la société qui a émis votre carte de crédit;
3. Réinitialisez les justificatifs d'identité associés à vos comptes, comme vos comptes de courriel ou de médias sociaux;
4. Signalez l'incident au Centre antifraude du Canada au 1-888-495-8501 ou à **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**.