Liste de vérification de la cybersécurité : opérations bancaires en ligne sécuritaires

Pour vous prémunir contre les cybercriminels, il est essentiel que vous fassiez preuve de vigilance. Bien que RBC soit résolue à protéger vos renseignements financiers, vous pouvez prendre quelques simples mesures pour rehausser votre protection encore davantage.

1. Authentification à deux facteurs ou multifacteur sur votre application mobile

Ce que vous pouvez faire :

❑ Enable 2-step verification in the RBC Mobile app. This will help ensure it's only you who has access to your bank accounts online.

2. Dépôt automatique des télévirements

Ce que vous pouvez faire :

❑ Grâce au Dépôt automatique Virement Interac, vous n'avez pas à ouvrir une session dans Banque en direct ou à répondre à une question d'identification personnelle pour recevoir un télévirement. Ce service élimine les questions d'identification auparavant requises pour chaque opération, ce qui réduit les risques d'interception.

3. Verrouillage de carte

Ce que vous pouvez faire :

❑ Vous pouvez bloquer votre carte client ou carte de crédit RBC temporairement en tout temps. Si vous égarez votre carte, il vous suffit d'ouvrir une session dans l'appli Mobile RBC et de la bloquer à la page des détails de votre compte.

4. Alertes

Des alertes peuvent vous être envoyées gratuitement afin de vous aider à gérer votre argent et à savoir constamment où vous en êtes. Transmises en temps quasi réel, elles portent sur telle ou telle activité menée dans vos comptes. Vous pourriez ainsi éviter des frais imprévus ou des frais d'intérêt, en plus de détecter rapidement d'éventuelles activités inhabituelles.

Ce que vous pouvez faire :

❑ Vous pouvez personnaliser facilement vos alertes dans RBC Banque en direct ou dans l'appli Mobile RBC pour surveiller les opérations anormales.

5. Choix de questions d'identification personnelle sûres

Ce que vous pouvez faire :

❑ Si vous choisissez de ne pas activer le dépôt automatique, lorsque vous envoyez de l'argent par Virement Interac, assurez-vous que vos questions d'identification personnelle sont difficiles à deviner et évitez les réponses faciles à trouver en ligne ou sur les médias sociaux, comme le nom de votre animal de compagnie ou votre destination vacances préférée.

❑ N'indiquez jamais la réponse à la question dans le message qui accompagne le virement.

6. Utilisation d'une connexion Internet sécurisée

Évitez d'utiliser les points d'accès sans fil, surtout si vous accédez à des comptes contenant de l'information confidentielle ou sensible, comme votre compte bancaire.

Ce que vous pouvez faire :

❑ Évitez de vous connecter à des comptes contenant de l'information confidentielle ou sensible.

❑ Utilisez un réseau privé virtuel (VPN) sécurisé et chiffré.

❑ Portez attention aux personnes qui vous entourent et qui peuvent regarder par-dessus votre épaule.

7. Recours à des mots de passe sûrs et complexes

Il est essentiel d'utiliser des mots de passe sûrs pour protéger vos comptes en ligne. Les mots de passe constituent souvent la première ligne de défense contre les cybercriminels. Ils protègent vos renseignements personnels, comme vos comptes bancaires, les données sur votre santé ou vos documents privés, afin qu'ils ne tombent pas entre de mauvaises mains.

Ce que vous pouvez faire :

❑ Ne communiquez jamais vos mots de passe à qui que ce soit

❑ N'utilisez pas votre mot de passe de Banque en direct pour un autre compte. Bien qu'il soit préférable de ne jamais réutiliser les mots de passe, il est particulièrement important de redoubler de prudence lorsqu'il s'agit d'informations sensibles comme dans le cas de votre compte bancaire.

❑ Plus un mot de passe est long, plus il est fiable. Les experts recommandent de créer des mots de passe comportant au moins 12 caractères, idéalement 16.

❑ Réinitialisez périodiquement vos mots de passe.

8. Examinez périodiquement vos relevés de compte

Ce que vous pouvez faire :

❑ Passez régulièrement en revue vos relevés bancaires : la présence d'achats inconnus peut être un signe d'usurpation de votre identité.

9. Protégez vos renseignements personnels

Ne donnez pas de renseignements personnels à quelqu'un que vous ne connaissez pas, même si la personne prétend être d'une société de confiance ou de votre banque.

Ce que vous pouvez faire :

❑ Même si le message semble convaincant, ne communiquez jamais à quiconque votre NIP, votre mot de passe, vos numéros de compte ou votre code d'accès à usage unique. Votre banque ne vous demandera jamais de lui fournir de tels renseignements..

❑ Raccrochez ou supprimez le message et ne cliquez sur aucun lien. .

❑ Ne vous fiez pas à l'identité de l'appelant : les escrocs sont doués pour mystifier les numéros de téléphone, alors ne vous laissez pas duper par un numéro qui ressemble à celui de votre banque.

❑ Communiquez directement avec votre banque en utilisant le numéro de téléphone qui figure au verso de votre carte de crédit ou de débit.

10. Assurez-vous de parler à un agent de RBC

- Sachez que RBC ne vous demandera jamais de communiquer à qui que ce soit votre identifiant d'utilisateur, votre NIP, votre mot de passe ou un code à usage unique par texto, par courriel ou par messagerie vocale.
- Nous ne vous demanderons jamais d'ajouter un bénéficiaire RBC aux fins de vérification ni d'effectuer une opération au nom de RBC.
- Nous ne vous demanderons jamais non plus de télécharger une application d'accès à distance.
- À tout moment, si vous n'êtes pas certain de parler à un véritable conseiller RBC, raccrochez (ou ignorez le texto ou le courriel), puis appelez-nous ou rendez-vous en succursale dès que possible.
- Pour obtenir des mises à jour périodiques sur les escroqueries courantes et télécharger notre liste de vérification simple sur la sécurité en ligne, allez à rbc.com/cyber.

11. Signalez immédiatement la perte ou le vol de vos cartes de crédit ou de débit

Ce que vous pouvez faire :
❑ Si vous avez perdu votre carte de crédit ou de débit ou qu'elle a été volée, signalez-le immédiatement à RBC et verrouillez la carte dans l'appli Mobile RBC

Signalez toute fraude

Si vous croyez que vos renseignements personnels ont été volés ou obtenus par des moyens frauduleux en ligne, par téléphone ou par tout autre moyen, téléphonez-nous immédiatement.

N'hésitez pas à nous appeler si vous avez des questions ou des commentaires d'ordre général concernant la protection des renseignements personnels et la sécurité.
1 800 769-2511 (services bancaires par téléphone)
1 800 769-2555 (services bancaires mobiles et en ligne)
1 800 769-2512 (cartes de crédit)
1 800 769-2535 (Centre de soutien clientèle, Services bancaires en ligne RBC Express)