Liste de vérification sur la cybersécurité à l'intention des aînés

Avec la montée du cybercrime partout dans le monde, il importe plus que jamais de s'informer et d'informer ses proches sur les façons d'assurer sa cybersécurité. **La présente liste de vérification vise à vous renseigner sur les façons de vous protéger, vous et votre famille, et de protéger vos actifs numériques.**

Protection liée aux mots de passe

Il n'est pas rare que des escrocs accèdent à vos renseignements ou s'introduisent dans vos comptes en ligne en devinant votre mot de passe. Nous sommes nombreux à utiliser des mots de passe faciles à retenir, comme « motdepasse » ou « 1234 ».

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.
- ❑ Utilisez l'authentification multifacteur. Bien que les mots de passe soient préférables à une absence de protection, vos données sont beaucoup mieux protégées si vous combinez un mot de passe avec l'authentification multifacteur.

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.

Ce que vous pouvez faire :

- ❑ Établissez un dépôt automatique des télévirements. Ce service élimine les questions d'identification auparavant requises pour chaque opération, ce qui réduit les risques d'interception.
- ❑ Activez la vérification en deux étapes dans l'appli Mobile RBC.
- ❑ Examinez périodiquement vos relevés de compte : la présence d'achats inconnus peut être un signe d'usurpation de votre identité.
- ❑ Signalez immédiatement la perte ou le vol de vos cartes de crédit ou de débit.
- ❑ Ne fournissez jamais de renseignements confidentiels, d'identifiants ou de mots de passe en réponse à un courriel, à un texto ou à un appel non sollicité.
- ❑ Évitez d'agir sous le coup de l'émotion ou d'un sentiment d'urgence.
- ❑ Activez les alertes sur compte pour surveiller les opérations anormales.

Escroquerie par courriel

L'escroquerie par courriel est une forme très répandue d'escroquerie en ligne. Au moyen d'un courriel, on tente d'amener des gens à fournir des renseignements personnels, financiers ou commerciaux. En général, le courriel hameçon présente au destinataire une situation urgente (« Votre compte bancaire a été suspendu »), fixe un délai (« Vous devez vérifier votre compte dans les 24 heures ») et contient un lien vers une page où le destinataire doit fournir des renseignements confidentiels (« afin de régler le problème »). L'hameçonneur peut ainsi obtenir des mots de passe, des numéros de compte ou des noms de clients, ou même accéder aux systèmes informatiques de sa victime. Rappelez-vous qu'une organisation légitime ne demande jamais de fournir des renseignements de cette manière.

Ce que vous pouvez faire :

- ❑ N'inscrivez jamais de renseignements personnels dans un courriel, notamment des numéros de compte, des dates d'anniversaire, des numéros d'assurance sociale et d'autres données sensibles.

❑ N'ouvrez pas les pièces jointes et ne cliquez pas sur les liens si vous n'en connaissez pas la source. Si vous recevez un courriel comportant une pièce jointe suspecte, ignorez-le et supprimez-le.

❑ Veillez à la sécurité de votre adresse courriel. Votre adresse courriel est personnelle : évitez de la publier sur des forums publics ou de la saisir sur des sites auxquels vous ne faites pas confiance. En outre, vous n'êtes pas tenu de la fournir à un employé d'un magasin qui vous la demande.

Escroqueries par téléphone et par message texte

Avez-vous déjà reçu un appel ou un texto d'un numéro que vous ne reconnaissez pas vous demandant de faire quelque chose, comme fournir des renseignements personnels ou financiers ? Il pourrait s'agir d'une tentative d'hameçonnage par texto.

Ce que vous pouvez faire :

❑ Ne répondez pas si vous ne reconnaissez pas le numéro.

❑ Ne donnez jamais de renseignements personnels à quelqu'un que vous ne connaissez pas.

❑ Méfiez-vous de l'usurpation de l'identité d'un petit-enfant. Il s'agit de l'une des escroqueries les plus répandues à l'heure actuelle : l'année dernière seulement, près de 10 millions de dollars ont été soutirés à des aînés canadiens de cette façon. Si vous recevez un appel d'une personne qui prétend être votre petite-fille ou votre petit-fils, ne tombez pas dans le panneau, surtout si elle vous demande de l'argent, une carte de crédit ou une carte-cadeau pour une situation d'urgence. Raccrochez et appelez directement un membre de votre famille.

❑ Ne cliquez pas sur les liens reçus de numéros que vous ne reconnaissez pas.

❑ Évitez d'agir sous le coup de l'émotion ou d'un sentiment d'urgence.

❑ Si le numéro n'est pas légitime, supprimez le texto de votre téléphone.

Paramètres de cellulaire

Les téléphones intelligents sont utiles, mais ils ne sont pas toujours sûrs. La sécurité de votre téléphone intelligent comporte deux volets : la protection de l'appareil lui-même (contre la perte ou le vol) et la protection des données qu'il contient.

Ce que vous pouvez faire :

❑ Désactivez la technologie Bluetooth lorsque vous ne l'utilisez pas.

❑ N'installez pas d'applications indiscrètes ou désinstallez-les si c'est déjà fait. En outre, désinstallez les applications que vous n'utilisez plus.

❑ Activez la fonction de localisation du téléphone pour pouvoir localiser votre appareil et protéger vos données en cas de perte.

❑ Activez l'authentification multifacteur pour les sites que vous visitez.

Sites Web simulés

Les escrocs créent de faux sites Web de magasins de détail qui ressemblent à de véritables sites. Toutefois, vous ne recevez pas la marchandise que vous y achetez.

Ce que vous pouvez faire :

❑ Achetez votre marchandise auprès d'entreprises ou de personnes que vous connaissez de réputation ou d'expérience.

❑ Lorsque vous passez à la caisse, assurez-vous que vous êtes toujours sur le site Web reconnu et que vous n'avez pas été redirigé vers une nouvelle page.

❑ Soyez plus vigilant si le vendeur est loin de chez vous ou s'il n'y a pas beaucoup d'avis publiés à son sujet.

❑ Vérifiez périodiquement vos relevés de carte de crédit pour repérer tout montant récurrent ou inconnu.

Signaler une 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)