Soyez cyberfuté

Guide de prévention de la fraude et de cybersécurité RBC

Apprenez à assurer la sécurité de vos actifs numériques pour vous protéger, vous, votre famille et votre entreprise.

L'information : meilleure protection contre la fraude

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. L'évolution rapide des technologies, notamment de l'intelligence artificielle générative, permet aux cybercriminels d'user de moyens inattendus pour vous escroquer à l'égard de vos actifs numériques.

Le présent guide vise à vous renseigner sur les façons de vous protéger, vous et votre famille, et de protéger vos actifs numériques.

À l'intérieur

Opérations bancaires en toute sécurité avec RBC

Grâce à la Garantie de sécurité des Services bancaires numériques RBC, vous êtes entièrement protégé relativement à toute opération que vous n'avez pas effectuée, que vous n'avez pas approuvée ou pour laquelle vous n'avez pas donné votre autorisation. Nous rembourserons intégralement toute opération non autorisée effectuée dans RBC Banque en direct ou l'appli Mobile RBC.

La protection de nos systèmes et des renseignements personnels de nos clients est toujours une priorité absolue. Afin de vous protéger lors de vos activités bancaires en ligne, nous vous encourageons à activer les fonctions de sécurité suivantes pour tous vos comptes en ligne :

Authentification à deux facteurs ou authentification multifacteur (lorsque c'est possible)

L'activation de l'authentification à deux facteurs ou de l'authentification multifacteur ajoute une couche supplémentaire de sécurité, car le système vérifie alors votre identité de deux façons ou plus : d'abord au moyen d'un mot de passe sûr, puis au moyen d'un code numérique ou d'un identifiant biométrique tel qu'une empreinte digitale.

Dépôt automatique des télévirements

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. Une fois que vous avez enregistré votre adresse courriel ou votre numéro de téléphone cellulaire, dès que quelqu'un vous envoie de l'argent, les fonds sont automatiquement déposés dans le compte désigné. Ce service élimine les questions d'identification auparavant requises pour chaque opération, ce qui réduit les risques d'interception.

Ce que vous pouvez faire

Les clients jouent eux aussi un rôle important dans la protection et la sauvegarde de leurs systèmes et de leurs comptes. Nous sensibilisons périodiquement nos clients aux meilleures pratiques, comme l'installation des mises à jour de logiciels, la protection des mots de passe et des comptes de messagerie, ainsi que la vigilance à l'égard de l'hameçonnage.

1. Choix de questions d'identification personnelle sûres

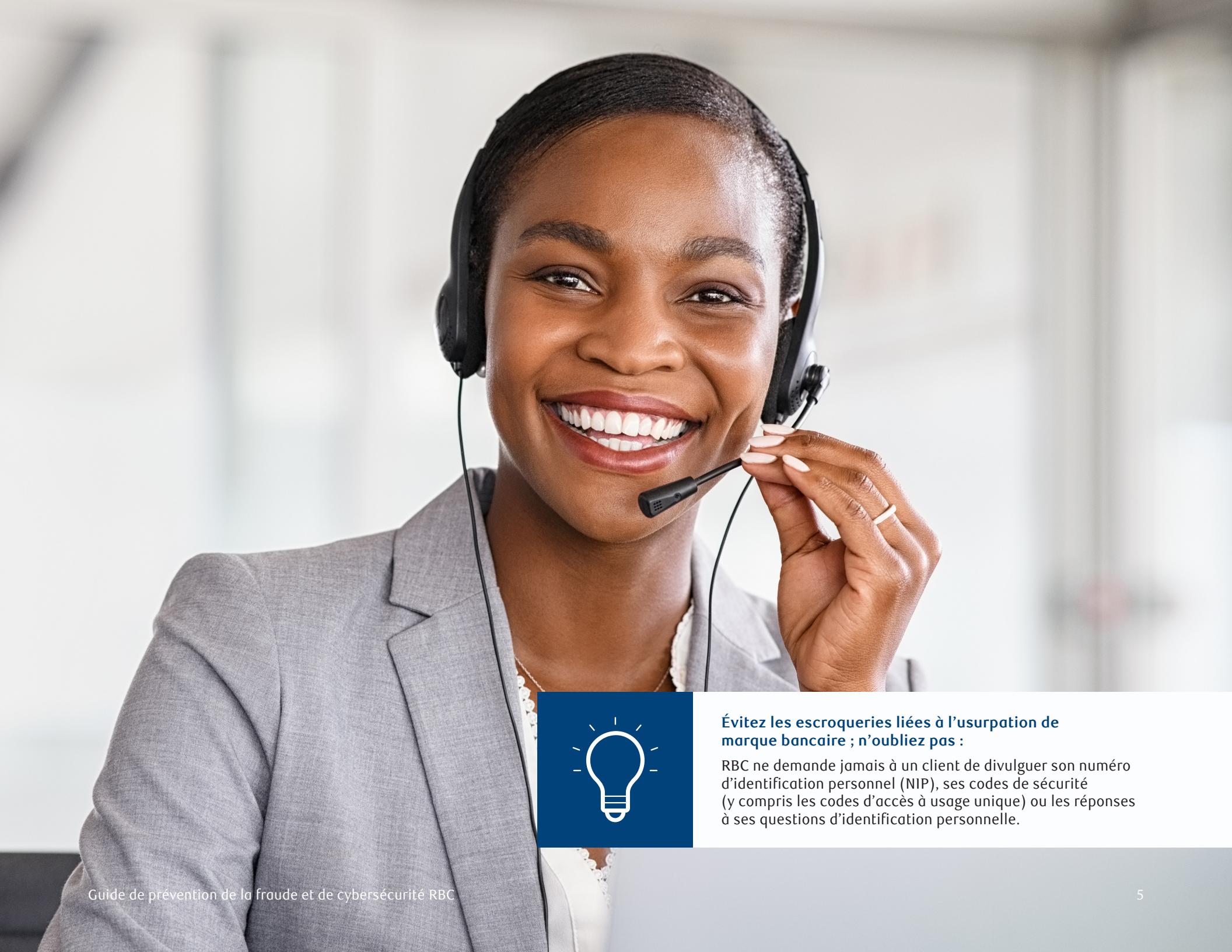
Si vous choisissez de ne pas activer le dépôt automatique, lorsque vous envoyez de l'argent par Virement *Interac*, assurez-vous que vos questions d'identification personnelle sont difficiles à deviner et évitez les réponses faciles à trouver en ligne ou sur les médias sociaux, comme le nom de votre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

2. 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.

3. 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.



Évitez les escroqueries liées à l'usurpation de marque bancaire ; n'oubliez pas :

RBC ne demande jamais à un client de divulguer son numéro d'identification personnel (NIP), ses codes de sécurité (y compris les codes d'accès à usage unique) ou les réponses à ses questions d'identification personnelle.

Prévention de la fraude et cybersécurité

Une protection dans le monde numérique pour soi et sa famille

Défini de façon large, le cybercrime englobe tous les crimes commis avec un ordinateur, que ce soit pour répandre un virus, voler de l'argent, usurper l'identité de quelqu'un ou mettre la main sur des données concernant des clients.

Bien que ce type de crime revête de nombreuses formes, voici les principaux types que vous devez connaître, ainsi que les moyens de les contrer.

Compromission de 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. En faisant des milliards de tentatives par seconde à l'aide de multiples ordinateurs, les criminels peuvent obtenir même des mots de passe relativement compliqués en quelques heures.
Nous sommes nombreux à utiliser des mots de passe faciles à retenir, comme « motdepasse » ou « 1234 ». Or, les escrocs le savent et donc, utiliser un tel mot de passe, c'est comme donner les clés de son domicile et son adresse à des étrangers.

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. S'il est préférable de ne jamais utiliser un même mot de passe pour plus d'un compte, il est particulièrement important de redoubler de prudence lorsqu'il s'agit d'un compte contenant de l'information sensible comme 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.

Hameçonnage

L'hameçonnage 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 (« Notre service d'audit a décelé un problème concernant votre compte »), 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.
- ☐ Méfiez-vous des fausses adresses courriel et des faux sites Web. Si un courriel semble étrange ou contient des fautes d'orthographe et de grammaire, il vaut mieux l'ignorer et le supprimer, même s'il est indiqué qu'il provient d'une entreprise légitime. De nombreux escrocs créent des adresses courriel et des sites Web qui semblent authentiques, mais qui ne le sont pas du tout.
- ☐ 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.

Hameçonnage vocal

Si vous recevez un appel d'une personne qui prétend travailler pour une source fiable et vous demande de fournir vos renseignements personnels et bancaires, il peut s'agir d'« hameçonnage vocal ».

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.

Hameçonnage par texto

Avez-vous déjà reçu d'un numéro que vous ne reconnaissiez pas un texto dans lequel on vous demandait de faire quelque chose, comme de fournir des renseignements confidentiels ou financiers ? Il pourrait s'agir d'hameçonnage par texto.

L'hameçonnage par texto est le fait pour un cybercriminel de vous envoyer un texto pour tenter d'obtenir vos renseignements personnels.

Ce que vous pouvez faire :

- ☐ 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.

Piratage psychologique

Le piratage psychologique est l'art de manipuler les gens pour qu'ils donnent des renseignements confidentiels. Les cybercriminels utilisent souvent cette tactique, qui joue sur les émotions, pour inciter leurs victimes à leur donner leurs mots de passe ou leurs renseignements bancaires, ou pour accéder à leur ordinateur afin d'y installer secrètement des logiciels malveillants.

Ce que vous pouvez faire :

- ☐ Ne fournissez jamais de renseignements confidentiels, d'identifiants ou de mots de passe en réponse à un courriel ou à un texto non sollicité.
- ☐ Évitez d'agir sous le coup de l'émotion ou d'un sentiment d'urgence.

Logiciel malveillant

Les logiciels malveillants (ou maliciels) sont conçus pour infiltrer des systèmes informatiques et causer des dommages, que ce soit en corrompant des fichiers ou des applications, en épiant des activités ou en copiant des données. Les cybercriminels se servent souvent de tels « outils » pour pénétrer dans des systèmes afin de voler de l'argent ou des renseignements. Une intrusion par logiciel malveillant est parfois perceptible à certains signes : lenteur du traitement, disparition de logiciels de protection, ou multiplication des pannes et des cas de gel d'écran.

Ce que vous pouvez faire :

- ☐ Installez un logiciel antivirus et maintenez-le à jour.
- ☐ Supprimez les applications que vous n'utilisez pas.
- ☐ Ne fournissez jamais de renseignements confidentiels, d'identifiants ou de mots de passe en réponse à un courriel ou à un texto non sollicité.

Rançongiciel

Le rançongiciel est l'un des nombreux types de logiciel malveillant. Nous en soulignons l'importance en raison de la fréquence croissante des attaques et du tort énorme qu'elles causent aux entreprises. L'ampleur des dommages tient au fait qu'une fois les systèmes infiltrés, le rançongiciel copie habituellement l'ensemble des fichiers, puis verrouille les systèmes. Les pirates exigent ensuite une rançon pour les déverrouiller. Ce genre d'attaque peut paralyser une entreprise et il peut falloir des semaines, voire plus, pour revenir à la normale. Dans l'intervalle, l'entreprise est parfois incapable d'exercer ses activités.

Ce que vous pouvez faire :

- ☐ Les mesures de prévention contre les logiciels malveillants sont également efficaces contre les rançongiciels. Toutefois, il ne suffit pas d'être vigilant dans l'utilisation des logiciels et du courriel ; il faut aussi faire régulièrement des copies de sécurité des données de l'entreprise pour qu'elle puisse reprendre rapidement ses activités en cas d'attaque par rançongiciel.

Usurpation d'identité

L'usurpation d'identité se produit lorsqu'un fraudeur accède à vos renseignements personnels (votre nom, votre date de naissance, votre numéro d'assurance sociale, etc.) et les utilise pour effectuer des opérations financières en votre nom. Il peut s'agir d'accéder à vos comptes, d'ouvrir de nouveaux comptes de cartes de crédit, de demander du crédit ou des prêts hypothécaires ou d'émettre des chèques en votre nom.

Les usurpateurs peuvent obtenir ces renseignements n'importe où : dans votre boîte aux lettres, par courriel, par téléphone, sur des relevés que vous avez jetés à la poubelle ou même sur le disque dur d'un vieil ordinateur dont vous vous êtes départis.

Ce que vous pouvez faire :

- ☐ Examinez périodiquement vos relevés de compte : la présence d'achats inconnus peut être un signe d'usurpation de votre identité.
- ☐ Ne communiquez jamais de renseignements personnels par courriel, notamment des numéros de compte, des dates d'anniversaire, des numéros d'assurance sociale et d'autres données sensibles.
- ☐ Signalez immédiatement la perte ou le vol de vos cartes de crédit ou de débit.

Médias sociaux

Les médias sociaux ont gagné en popularité auprès de tous les groupes d'âge, mais également auprès des escrocs.

S'il est relativement facile pour les escrocs d'entrer en contact avec les utilisateurs, il est également facile pour ces derniers de se protéger : il faut surtout savoir à quoi s'attendre et comment gérer ses paramètres.

Ce que vous pouvez faire :

- ☐ N'acceptez pas les demandes d'amitié de personnes qui vous sont étrangères.
- ☐ Évitez de publier de l'information sensible comme votre numéro de téléphone, votre adresse et même l'information concernant votre voyage lorsque vous partez en vacances, ou d'envoyer de tels renseignements en message privé.
- ☐ Activez tous les paramètres de protection des renseignements personnels. Ces paramètres sont personnalisables et il est préférable de choisir les options qui offrent le niveau de sécurité le plus élevé.
- ☐ Désactivez le géomarquage et la géolocalisation dans les paramètres de l'appareil. Le géomarquage permet aux cybercriminels, aux escrocs et à d'autres personnes malintentionnées de savoir où vous vous trouvez ; il pourrait aussi leur permettre de savoir où sont vos enfants.
- ☐ Méfiez-vous des fausses occasions de placement, en particulier celles qui s'appuient sur des endosseurs très connus.

Faux sites Web

Les escroqueries en ligne n'ont rien de nouveau, mais elles ne sont pas près de disparaître. 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.

Protection des données

Que ce soit à la caisse d'un magasin ou lors du téléchargement d'une application, vos données personnelles vous sont constamment demandées. Mais vous n'êtes pas tenu de les fournir. Vous n'êtes pas obligé de donner votre code postal, votre adresse courriel ou votre numéro de téléphone. Il est pertinent de se demander pourquoi un site Web ou une application vous demande de tels renseignements. Vos données ont une grande valeur : traitez-les comme telles.

Ce que vous pouvez faire :

- ☐ Refusez de vous inscrire aux infolettres ou désabonnez-vous : vous réduirez ainsi le nombre de personnes et d'organisations qui détiennent vos coordonnées.
- ☐ Utilisez l'authentification multifacteur, qui complique le vol de vos renseignements par des cybercriminels.
- ☐ Méfiez-vous des points d'accès sans fil.
- ☐ Gardez vos comptes de médias sociaux privés.

☐ Ne laissez pas les sites enregistrer vos renseignements, en particulier vos renseignements sur les paiements tels que les données de cartes de crédit et de débit.
☐ Parcourez les paramètres de protection des renseignements personnels.

Réseau privé virtuel (VPN)

Un VPN est un réseau privé virtuel. Lorsque le VPN est activé sur votre appareil, il établit une connexion sécurisée sur un réseau en ligne. L'utilisation d'un VPN est l'une des façons de préserver la confidentialité de vos données chaque fois que vous utilisez vos appareils.

Ce que vous pouvez faire :

☐ Procurez-vous un VPN. Téléchargez un VPN sur votre appareil, ouvrez une session avec le compte que vous avez créé, puis choisissez un serveur dans la liste des serveurs canadiens.

Authentification multifacteur

Il arrive que l'authentification multifacteur soit automatiquement activée, mais, dans certains cas, vous devez choisir de l'utiliser.

Ce que vous pouvez faire :

☐ Lorsque l'authentification multifacteur est offerte, utilisez-la. La plupart des plateformes populaires proposent cette option et vous pouvez l'activer dans vos paramètres.
☐ L'accès à l'appli Mobile RBC s'effectue désormais au moyen de la vérification en deux étapes pour une protection accrue. Ainsi, nous envoyons un message à l'appareil de confiance que vous avez choisi chaque fois qu'une personne tente d'ouvrir une session à partir d'un autre appareil. Dès lors, si vous n'êtes pas cette personne, vous pouvez empêcher un accès non autorisé à votre compte.
☐ Activez les alertes sur compte pour surveiller les opérations anormales.

Points d'accès sans fil

Les points d'accès sans fil sont moins sûrs que votre réseau privé, car vous ne savez ni qui les a installés ni qui s'y connecte.

Ce que vous pouvez faire :

☐ Évitez de vous connecter à des comptes contenant de l'information confidentielle ou sensible.
☐ Utilisez un VPN sécurisé et chiffré.
☐ Portez attention aux personnes qui vous entourent et qui peuvent regarder par-dessus votre épaule.

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.

Le saviez-vous ?

Le Centre antifraude du Canada estime que les escroqueries en ligne comptent pour plus de 70 % des fraudes.

Escroqueries en ligne

Aperçu des types d'escroquerie les plus courants

En bref, les escroqueries sont en hausse. Certaines sont cependant plus populaires que d'autres.

Escroqueries par courriel (hameçonnage)

55 % des répondants ont vécu une tentative de fraude par courriel qui semblait provenir d'une source légitime et qui les dirigeait vers un faux site Web[1].

Escroqueries par téléphone (hameçonnage vocal)

Dans 47 % des cas, la fraude signalée a été effectuée au moyen d'un appel téléphonique pendant lequel un escroc a tenté d'inciter la victime à communiquer de l'information sensible[1].

Escroqueries par texto (hameçonnage par texto)

40 % des répondants ont reçu des textos frauduleux qui tentaient de les amener à fournir de l'information sensible[1].

Les tactiques d'hameçonnage par courriel, d'hameçonnage vocal et d'hameçonnage par texto exploitent des événements d'actualité (comme les efforts de secours en Ukraine et la COVID-19) ou créent des messages qui semblent provenir d'organismes de confiance ou de personnes que vous connaissez.

Voici les escroqueries les plus courantes et les moyens de s'en prémunir.

1. Gouvernement (fédéral, provincial et municipal) :

Faux courriels, appels ou textos provenant d'escrocs qui se font passer pour des représentants de l'Agence du revenu du Canada et qui exigent un paiement immédiat, à défaut de quoi la victime pourrait être arrêtée ou emprisonnée.

2. Services de livraison :

Postes Canada et UPS font partie des prestataires de services de livraison desquelles il est le plus courant qu'un fraudeur prétende être un représentant, demandant à obtenir un paiement ou des renseignements d'un client avant de pouvoir effectuer la livraison.

3. Commerce de détail :

Par exemple, un escroc communique avec vous en se faisant passer pour un représentant d'Amazon, puis prétend qu'il y a un problème avec une commande récente et que vous avez droit à un remboursement. Le hic, c'est que pour pouvoir recevoir votre remboursement, vous devez cliquer sur un lien vers un autre site Web ou fournir vos renseignements personnels.

4. Santé :

Les escroqueries liées aux vaccins et aux trousses de test pour la COVID-19 et d'autres virus sont toujours en circulation.

5. Finances :

Un fraudeur vous envoie un courriel vous avisant que votre compte bancaire a été bloqué et que vous devez entrer vos justificatifs d'ouverture de session afin de pouvoir le déverrouiller et accéder à vos fonds.

Conseil :

Connaître les types de fraudes en ligne et les indices permettant de les déceler est la clé pour vous protéger des cybercriminels. Rendez-vous sur **rbc.com/alertesdefraude** pour découvrir les escroqueries en ligne qui visent actuellement les clients de RBC.

Les escrocs sont de plus en plus créatifs : il est de plus en plus difficile de détecter une escroquerie. Vous devez vraiment rester vigilant. Votre meilleur atout consiste à prendre des mesures actives pour vous protéger : mettre des alertes en place, activer l'authentification multifacteur, utiliser des mots de passe uniques (en particulier pour les services bancaires). Finalement, souvenez-vous que vous ne devez jamais communiquer vos renseignements financiers personnels.

Kevin Purkiss, vice-président, Lutte antifraude

Escroqueries courantes

Courriel

Votre versement est prêt à être effectué.
Cliquez pour l'accepter : tiny.cc/ylayuz

Texto

Malheureusement, notre livreur n'a pas pu obtenir de signature pour votre colis. Afin d'éviter tout retard supplémentaire, remplissez sans tarder la demande de nouvelle livraison. Pour en savoir plus, consultez le site serv1postcanada.imfo.

Courriel

Veuillez réinitialiser votre mot de passe.
Cliquez pour accepter : tiny.cc/ylayuzt

Texto

Votre abonnement à Netflx a été suspendu, car il semble y avoir des problèmes avec vos renseignements de facturation. Pour utiliser votre compte, veuillez cliquer sur ce lien et suivre les directives : Netfix-reactivatemyacount.com.

Planification et gestion

Gestion des incidents de cybersécurité

Les petites comme les grandes entreprises font souvent l'erreur de ne s'attarder qu'à la prévention. Pourtant, les incidents de cybersécurité ne sont pas qu'une possibilité théorique, mais bien une réalité qui touchera tôt ou tard votre entreprise. Une bonne gestion des cybercrises – avant, pendant et après l'incident – permet souvent d'en atténuer les répercussions. Le tout repose d'abord sur une planification efficace. L'élaboration d'un plan de gestion des incidents de cybersécurité est la première mesure à prendre pour réduire le cyberrisque. Même s'il n'existe pas de plan universel, toutes les entreprises ont intérêt à suivre certaines règles de base en matière de cybersécurité.

Élaboration d'un plan de gestion de crise de cybersécurité

Pour bien gérer un incident de cybersécurité, le plus important, c'est d'avoir un plan en place. Cette planification peut sembler défaitiste, mais dans un environnement numérique en constante évolution, la planification fait partie de toute bonne stratégie de gestion du risque et d'intervention en cas d'incident.

Vous pouvez faire appel à une entreprise spécialisée ou à votre propre personnel des TI pour élaborer et tester votre plan de gestion, mais la direction et les divers services de l'entreprise doivent y collaborer, car les incidents de cybersécurité signalent un problème à l'échelle de l'organisation.

Un bon plan de gestion de crise de cybersécurité comprendra les éléments suivants :

Équipe de gestion des incidents

Nous considérons souvent la cybersécurité comme la responsabilité de l'équipe de la technologie de l'information (TI), mais il faut un large éventail d'aptitudes pour gérer un incident de cybersécurité. Selon la taille de l'entreprise, l'équipe de gestion peut réunir du personnel de divers services : TI, services juridiques, communications, exploitation, etc.

Plans d'intervention selon divers scénarios

Une fois déterminés les risques les plus importants, élaborez un plan pour chacun en recensant les ressources de gestion nécessaires. S'il vous manque certaines ressources à l'interne, déterminez comment vous comblerez vos lacunes en cas d'incident.

Plan de communication détaillé

Répertoriez les parties prenantes à aviser en cas d'incident et déterminez à quelle étape et de quelle façon vous devez les informer. Ces parties prenantes comprennent vos clients, vos investisseurs et vos partenaires. Vous devez aussi déterminer comment vous recueillerez et fournirez les renseignements requis par les autorités chargées de l'application des lois et les autorités réglementaires, le cas échéant. Sur le plan de la réputation, des communications régulières et transparentes vous permettront de garder le contrôle sur l'information véhiculée afin de prévenir les conjectures.

Révisions périodiques

Puisque les cybercriminels trouvent chaque jour de nouvelles façons de commettre des délits, les menaces potentielles se multiplient. Par conséquent, votre plan de gestion doit être révisé périodiquement pour tenir compte des nouvelles menaces. Vous devez aussi le tester pour vous assurer qu'il demeure efficace.

Approche axée en priorité sur le client

Votre plan de gestion de crise de cybersécurité devrait viser à protéger vos clients en priorité. Il faut donc planifier des communications proactives, fréquentes et transparentes avec vos clients afin de les renseigner sur les répercussions des incidents et de répondre rapidement et précisément à leurs questions.

Mise en œuvre

Pour vous faciliter la tâche, nous avons conçu une grille de gestion de crise de cybersécurité que vous pouvez télécharger ici. Elle vous aidera à vous préparer aux incidents éventuels, à réduire certains risques et à vous rétablir plus rapidement après un incident.

Les délits informatiques font partie des menaces auxquelles les entreprises doivent se préparer pour ne pas être prises de court. L'élaboration d'un plan de gestion peut vous permettre de réagir plus rapidement, d'atténuer les conséquences juridiques ou les atteintes à la réputation de votre entreprise, et de protéger votre relation avec vos clients.

Doublez les mesures de sécurité
C'est un peu comme de poser plusieurs serrures sur votre porte.

Il n'existe pas d'approche universelle pour se protéger et protéger son entreprise. Il est important de donner de l'information sur le cybercrime et de faire de la sensibilisation sur le sujet, afin que chacun comprenne mieux l'incidence de ses gestes sur la posture de sécurité de son bureau de gestion de patrimoine familial. La solidité d'un système de sécurité dépend de celle de son maillon le plus faible.

Adam Evans, premier vice-président et chef de la sécurité de l'information, Cybersécurité mondiale RBC

Planification et gestion – Liste de vérification

Gestion des incidents de cybersécurité

Choix technologiques axés sur la sécurité

☐ Utilisation d'un système d'exploitation axé sur la sécurité
☐ Installation d'un logiciel antivirus
☐ Installation d'un pare-feu
☐ Installation des correctifs requis aux logiciels
☐ Désactivation de toute fonction de partage des données inutile
☐ Sauvegarde des systèmes et des données
☐ Stockage hors site des sauvegardes des systèmes et des données

Réseaux au bureau

Séparation des réseaux :
☐ Modification des données par défaut du réseau
☐ Recours à des mots de passe sûrs
☐ Configuration masquée du réseau principal du bureau
☐ Configuration d'un réseau distinct pour les appareils de l'Internet des objets (caméras, thermostat, équipement audiovisuel, électroménagers, etc.)
☐ Création d'un réseau d'invité (au besoin)

Appareils individuels sur le réseau :

☐ Confirmation que les logiciels sont à jour
☐ Confirmation que les micrologiciels sont à jour

Accès à distance :

☐ Non-utilisation, dans la mesure du possible, des points d'accès sans fil
☐ Configuration et utilisation d'un réseau privé virtuel (VPN)

Sécurité des appareils mobiles

☐ Téléchargement et utilisation de l'appli Mobile RBC
☐ Désactivation du Wi-Fi et de la technologie Bluetooth (lorsqu'ils ne sont pas utilisés)
☐ Établissement d'un mot de passe sûr ou d'identifiants biométriques pour déverrouiller ses appareils
☐ Installation d'un VPN
☐ Installation immédiate des mises à jour
☐ Désinstallation des applications qui sont inutilisées ou qui envoient automatiquement des données
☐ Suppression périodique des paramètres réseau pour que l'appareil oublie tout réseau non sécurisé précédemment utilisé
☐ Exécution d'une réinitialisation d'usine de ses appareils avant de les retourner ou de les faire réparer
☐ Activation de la fonction de localisation du téléphone (qui permet de supprimer à distance les données de l'appareil en cas de perte ou de vol)
☐ Désactivation de l'accès des développeurs (pour les appareils Android seulement)
☐ Programmation de sauvegardes chiffrées périodiques
☐ Configuration du stockage infonuagique automatique selon le niveau auquel vous êtes à l'aise avec les données partagées

Conformité et protection des renseignements personnels (revue périodique)

☐ Inventaire des appareils
☐ Information sur l'utilisation des appareils
☐ Information sur le réseau
☐ Impression des journaux
☐ Sécurité physique (secteurs protégés, armoires verrouillées, écrans verrouillés, déchiquetage des documents, etc.)

Gestion des mots de passe

- ☐ Mots de passe uniques pour chaque application ou service
- ☐ Utilisation du nombre maximal de caractères permis lors de la création des mots de passe
- ☐ Non-recours à des mots communs (p. ex., mot de passe)
- ☐ Non-recours à des enchaînements évidents (p. ex., Été2023!)
- ☐ Activation de l'authentification multifacteur (lorsque c'est possible)
- ☐ Détermination de la pertinence de renforcer la sécurité au moyen d'un gestionnaire des mots de passe, d'un jeton physique ou d'une clé FIDO

Préparation plus poussée

- ☐ Plan d'intervention en cas d'incident
- ☐ Exercice de sensibilisation et exercice sur table

N'oubliez pas que s'il est facile d'avoir une bonne posture de sécurité, en faire une habitude demande des efforts. Toutefois, une telle habitude peut vous éviter bien des tracas, à vous et à votre entreprise. En effet, dans notre monde de plus en plus interconnecté et numérisé, la question n'est pas de savoir « si », mais « quand » vous serez confronté à un cyberincident.

Adam Evans, premier vice-président et chef de la sécurité de l'information, Cybersécurité mondiale RBC

Points à retenir

Mesures pour maintenir une longueur d'avance

La sensibilisation et l'information constituent les meilleurs moyens de défense contre le cybercrime.

Même si vous ne pouvez pas vous tenir au fait de toutes les escroqueries utilisées, le fait de connaître les types de menaces et de risques qui existent peut vous aider à vous protéger.

Soyez cyberfuté :

1. Ne répondez pas au téléphone si vous ne reconnaissez pas le numéro. Si l'appelant est quelqu'un que vous connaissez réellement, il laissera un message ou vous enverra un texto expliquant la nature de son appel.

2. Ne donnez pas de renseignements personnels à quelqu'un que vous ne connaissez pas. Même si la personne prétend appartenir à une société ou à un organisme de confiance, raccrochez si elle vous demande des renseignements personnels.

3. N'ouvrez pas les pièces jointes si vous ne connaissez pas la source. Si vous recevez un courriel comportant une pièce jointe suspecte, supprimez-le.

4. Soyez conscient que les entreprises et institutions financières légitimes ne vous demanderont pas de mettre à jour votre compte ni de fournir des renseignements de connexion par texto. Confirmez toute demande reçue par texto en appelant l'organisation au moyen de son numéro de téléphone officiel.

5. Méfiez-vous des fausses adresses courriel et des faux sites Web. Si un courriel semble étrange ou s'il contient des fautes d'orthographe ou des erreurs de grammaire alors qu'il prétend provenir d'une entreprise légitime, il est préférable de simplement le supprimer. De nombreux escrocs créent des adresses courriel et des sites Web qui semblent authentiques, mais qui ne le sont pas du tout.

6. Sur les médias sociaux, acceptez uniquement les demandes d'amitié et d'abonnement des personnes que vous connaissez.

La sensibilisation et l'information sont la clé de la sécurité. Prenez un moment pour vous familiariser avec les plus récentes menaces et tactiques afin de vous protéger, vous et vos proches.

rbc.com/alertesdefraude

Certains indices sont à surveiller : mention de n'en parler à personne, demande d'envoi d'argent par des moyens inhabituels, recommandation de mettre des bitcoins sur un compte particulier… Souvenez-vous que si une offre semble trop belle pour être vraie, c'est probablement une escroquerie !

Kevin Purkiss, vice-président, Lutte antifraude

Ressources supplémentaires

RBC	• Cyberfraude et meilleures pratiques : www.rbc.com/cyberfute • Information sur les plus récentes escroqueries touchant les clients de RBC : rbc.com/alertesdefraude
Centre antifraude du Canada	www.centreantifraude.ca
Bureau de la concurrence Canada	www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/accueil
GRC – Escroqueries et fraudes	www.grc-rcmp.gc.ca/fr
Association des banquiers canadiens	Prévention de la fraude – Association des banquiers canadiens (cba.ca)

Signalement d'une cyberfraude à RBC

Si vous pensez avoir été victime d'une attaque par un logiciel malveillant ou que vos comptes ont été compromis, consultez la page Signaler une fraude à RBC pour obtenir nos coordonnées et communiquer avec nous immédiatement. Notre équipe d'experts dévoués vous indiquera les mesures appropriées à prendre.

Glossaire

Authentification multifacteur	Méthode d'authentification électronique qui demande à l'utilisateur de présenter au moins deux éléments pour s'identifier et avoir accès à une application ou à un compte. On parle parfois d'authentification à deux facteurs.
Cheval de Troie d'accès à distance	Programme qui permet à un intrus de prendre le contrôle d'un ordinateur afin d'exécuter des activités malveillantes.
Chiffrement	Brouillage des données afin que seuls les utilisateurs autorisés puissent comprendre l'information. Il s'agit d'un moyen de protéger ses données sur son réseau.
Courriel d'affaires compromis	Escroquerie dans le cadre de laquelle un message semblant provenir d'une source légitime (p. ex., le chef de la direction ou un haut dirigeant) incite le destinataire à prendre des mesures immédiates comme virer des fonds ou fournir des renseignements.
Gestionnaire des mots de passe	Base de données chiffrée recensant des mots de passe, qui peut être déverrouillée à l'aide d'un mot de passe principal.
Géomarquage	Ajout de coordonnées géographiques ou de données sur l'emplacement à divers médias, permettant ainsi à quiconque de savoir où une personne se trouve.
Hameçonnage par texto	Type d'hameçonnage qui cible les cellulaires. Ce type d'escroquerie utilise des textos pour inciter une personne à cliquer sur des liens ou à télécharger des pièces jointes qui installeront des logiciels malveillants ou tenteront de voler ses renseignements personnels ou financiers.
Hameçonnage vocal	Technique consistant à escroquer une personne par téléphone, en l'incitant à divulguer de l'information sensible.
Harponnage	Type d'hameçonnage qui cible un individu en particulier. Les messages peuvent ressembler à ceux d'un de ses amis ou d'un membre de sa famille et contenir des renseignements sur lui ou sur les organisations avec lesquelles il fait affaire.
Identifiant de réseau sans fil	Terme technique désignant le nom d'un réseau Wi-Fi.

Logiciel espion	Logiciel conçu pour s'infiltrer dans un appareil, recueillir des données et les transmettre à un tiers. Ce type de logiciel peut être malveillant, mais il peut aussi s'agir d'un logiciel légitime qui surveille les données à des fins commerciales, notamment pour la publicité.
Logiciel malveillant	Programme informatique conçu par des cybercriminels pour subtiliser de l'information, endommager des fichiers enregistrés ou prendre le contrôle d'un ordinateur ou d'un autre appareil.
Paiement pair à pair	Système de paiement lié au compte bancaire ou à la carte de crédit de l'utilisateur et qui permet à ce dernier d'envoyer et de recevoir des fonds de son appareil mobile.
Pare-feu	Dispositif de sécurité de réseau surveillant le flux de données entre deux réseaux. Il autorise ou bloque le passage de données selon un ensemble défini de règles de sécurité.
Phrase d'identification	Groupe de mots choisis de façon aléatoire, qui est facile à retenir pour l'utilisateur, mais difficile à deviner pour un pirate informatique (p. ex., Délai Éléphant Achat).
Piratage psychologique	Tromperie qui vise à manipuler une personne afin qu'elle divulgue des renseignements confidentiels ou personnels, qui pourront ensuite être utilisés à des fins frauduleuses.
Rançongiciel	Logiciel malveillant conçu pour bloquer l'accès à un ordinateur jusqu'à ce qu'une rançon soit payée.
Réseau Wi-Fi d'invité	Point d'accès d'un réseau distinct de celui auquel les principaux appareils du propriétaire se connectent. Un tel réseau permet de fournir un accès Internet à des appareils qui risquent plus d'avoir été exposés à des virus tout en s'assurant qu'ils ne se connectent pas à son réseau domestique.
Réseau privé virtuel (VPN)	Groupe d'ordinateurs ou de réseaux qui fonctionnent ensemble sur Internet afin de sécuriser les communications, notamment en les chiffrant.
Terminal de paiement spécialisé	Dispositif sous gestion indépendante utilisé dans un but particulier, par exemple à un kiosque, aux caisses d'un commerce de détail ou à un GAB (guichet automatique bancaire).

Pour en savoir plus sur la cybersécurité, consultez le site **rbc.com/cyberfute**

Sources :
[1] Centre antifraude du Canada, 2023.