**Comment puis-je protéger mon entreprise des menaces ?**

Les cas d'hameçonnage par courriel, par téléphone et d'autres attaques semblables sont en hausse. Les fraudeurs conçoivent des techniques de plus en plus sophistiquées pour soutirer de l'information de leurs victimes ; il est donc plus important que jamais de redoubler de prudence dans l'utilisation des services bancaires en ligne.

Si vous croyez avoir reçu un courriel ou appel téléphonique d'hameçonnage qui semble provenir de RBC :

Courriel :

1. Ne suivez pas les directives contenues dans le courriel, et ne cliquez sur aucun des liens.
2. Transférez-le immédiatement à phishing@rbc.com, puis supprimez-le.

Appel téléphonique :

1. Si la personne prétend vous appeler de RBC ou être un employé de RBC, et qu'elle vous demande des renseignements personnels, comme votre NIP ou la valeur de votre jeton RSA SecurID, raccrochez immédiatement.
2. Signalez l'appel au Centre de soutien clientèle, Services bancaires en ligne RBC Express, au **1 800 769-2535**.

**Important :** *Si vous soupçonnez quelqu'un de connaître votre identifiant utilisateur ou votre mot de passe pour ouvrir une session dans RBC Express, ou si votre jeton RSA SecurID est perdu ou a été volé, communiquez immédiatement avec votre administrateur des services ou avec RBC afin de faire verrouiller votre identifiant utilisateur.*

Pour parler au Centre de soutien clientèle, Services bancaires en ligne RBC Express, composez le **1 800 769-2535**.

**Comment reconnaître l'hameçonnage ?**

RBC ne vous demandera jamais votre mot de passe ou numéro de jeton des services RBC Express dans un courriel ou lors d'un appel téléphonique non sollicité. RBC Banque Royale ne vous enverra jamais de courriel ou de message vous demandant de donner, de confirmer ou de vérifier des renseignements personnels, de connexion ou de compte.

Les courriels hameçons et autres types d'hameçonnage sont de plus en plus raffinés et peuvent être difficiles à détecter. Pour apprendre à repérer les courriels hameçons et les faux sites Web, lisez les conseils à la rubrique « Comment les démasquer » du Centre d'information sur l'hameçonnage de RBC.

**À quoi ressemble l'hameçonnage ?**

**2Exemple 1**

Un employé reçoit un courriel qui semble provenir de RBC Banque Royale. Ce courriel peut être accompagné du bon logo et contenir un motif apparemment crédible, comme une demande de confirmation de renseignements ou d'approbation d'une opération bancaire. Généralement, ce type de courriel contient des liens qui semblent être ceux qui mènent vers les sites Web de la Banque. Le courriel hameçon peut même contenir un lien direct vers ce qui semble être la page d'ouverture de session des services bancaires en ligne RBC Express. ***Une fois qu'on a cliqué sur ces liens, le fraudeur s'en sert pour accéder au contenu de l'ordinateur du destinataire.***

***Exemple 2***

Vous recevez un appel d'un imposteur qui prétend être un employé de RBC, et qui vous demande de lui fournir le numéro de votre jeton, sous prétexte que votre jeton ne serait pas « synchronisé ». L'afficheur du téléphone indique « RBC » et un numéro de téléphone valide de RBC y est associé. Sans le savoir, la victime fournit à un imposteur le numéro de son jeton par téléphone, et un paiement est immédiatement approuvé et décaissé. Les fraudes de ce type prennent souvent davantage de temps à détecter, ce qui rend plus difficile le recouvrement des fonds.

**Que puis-je faire d'autre pour protéger mon entreprise ?**

1. **Vérifiez toujours les instructions de paiement**
   Prenez toujours des mesures supplémentaires afin d'être certain de l'origine des instructions de paiement. Méfiez-vous autant des appels téléphoniques que des courriels dans lesquels on vous demande des renseignements confidentiels, et sachez que les renseignements relatifs à l'identification de l'appelant peuvent être falsifiés par le fraudeur de façon à ce qu'il semble que l'appel provient d'une personne ou d'une entreprise reconnue.

2. **Signalez les possibles intrusions**
   Avisez immédiatement votre administrateur des services si vous soupçonnez quelqu'un de connaître votre ID d'ouverture de session ou votre mot de passe, ou en cas de perte ou de vol de votre jeton RSA SecurID. L'administrateur des services doit aviser RBC immédiatement.

   *Pour parler au Centre de soutien clientèle, Services bancaires en ligne RBC Express, composez le **1 800 769-2535**.*

3. **N'oubliez pas de fermer votre session**
   Vous devez toujours fermer la session et votre navigateur. Ainsi, personne d'autre ne pourra accéder à votre séance de services bancaires en ligne.

4. **Protégez votre mot de passe et votre jeton**
   Utilisez toujours un mot de passe difficile à deviner et le changer souvent. Protégez votre numéro de jeton. Ne révélez jamais votre mot de passe ou votre numéro de jeton à qui que ce soit.

5. **Méfiez-vous des fenêtres contextuelles, en particulier celles qui demandent des renseignements financiers ou d'identification.**
   Évitez de cliquer sur des boutons qui vous invitent à prendre des actions dans une fenêtre suspecte.

6. **Protégez votre ordinateur**
   Pour protéger vos logiciels, il est très important de vérifier fréquemment votre système d'exploitation et d'appliquer les réparations et les mises à jour fournies dans les sites Web du distributeur de votre navigateur.

7. **Utilisez un logiciel antivirus**
   Les logiciels antivirus offrent une protection contre les virus qui peuvent sournoisement endommager votre ordinateur. Veillez à utiliser un logiciel antivirus récent qui peut détecter les virus dans vos fichiers et vos courriels.

8. **Utilisez un pare-feu**
   Les pare-feu servent de barrière entre votre ordinateur et le reste du réseau Internet. Ils vous protègent contre les attaques malveillantes et bloquent le passage de certains types de données dans votre ordinateur.

9. **Utilisez un logiciel anti espion**
   Les logiciels anti espion bloquent l'installation sournoise de logiciels indésirables dans votre ordinateur. Un logiciel anti espion permet également d'éviter le ralentissement du fonctionnement des ordinateurs.

10. **Utilisez un logiciel anti pourriel**
    Les pourriels constituent une source croissante de virus informatiques. Utilisez des logiciels anti pourriel récents en plus des logiciels antivirus. Si vous recevez des pourriels, suivez la consigne suivante : n'essayez pas, n'achetez pas et ne répondez pas. Supprimez-les.

**Meilleures pratiques RBC Express**

Les services bancaires en ligne RBC Express allient la commodité des services bancaires en ligne aux caractéristiques de sécurité à la fine pointe conçues pour protéger votre entreprise et votre information financière. Vous pouvez tirer parti de ces caractéristiques de sécurité et des étapes décrites ci-dessus pour mieux protéger votre entreprise.

Le « Guide sur la sécurisation de vos opérations bancaires en ligne » est disponible sur le site du Centre-ressource, une fois que vous avez ouvert une session des services bancaires en ligne RBC Express. Vous y trouverez des explications sur les caractéristiques de sécurité obligatoires et facultatives offertes par les services bancaires en ligne RBC Express. Le Guide contient aussi les options recommandées et des conseils pratiques qui vous permettront de vous assurer que votre entreprise tire pleinement parti de toutes les caractéristiques de sécurité offertes. RBC recommande à votre entreprise de consulter régulièrement ce guide, afin qu'elle tire le maximum des caractéristiques de sécurité les plus récentes qui lui conviennent le mieux.

Si vous avez des questions sur les caractéristiques de sécurité qui conviennent le mieux à votre entreprise, veuillez communiquer avec votre représentant RBC.