Le petit livre des grandes fraudes

Guide sur la prévention des fraudes dans les petites et moyennes entreprises

rbc.com/cyberfute/entreprise

RBC®

La cybersécurité est une responsabilité partagée. Nous avons tous un rôle à jouer pour nous protéger. Des copropriétaires aux directeurs, en passant par les employés et les contractuels, nous devons tous collaborer pour renforcer nos défenses en cybersécurité.

1/5

des entreprises canadiennes ont dit avoir été victimes d'un incident de cybersécurité ayant eu des conséquences sur leurs activités en 2017

41 %

des grandes entreprises ont signalé des cyberincidents

28 %

des moyennes entreprises ont signalé des cyberincidents

19 %

des petites entreprises ont signalé des cyberincidents[1]

Table des matières

[1] Les statistiques ci-dessus sont tirées de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2017.

Message de **Laurie Pezzente**

Chef de la sécurité et première vice-présidente, Cybersécurité mondiale, Banque Royale du Canada (RBC)

Message de **Shawna Coxon**

Chef adjointe, Service de police de Toronto

Il est facile de croire qu'une petite ou moyenne entreprise n'est pas assez importante pour attirer l'attention des cybercriminels. Toutefois, le cybercrime s'intéresse bel et bien aux entreprises plus petites pour diverses raisons : leurs ressources technologiques sont souvent limitées, elles sont liées à de plus grandes entreprises, elles détiennent des renseignements de grande valeur et elles ont de l'argent.

Les fraudeurs adaptent leurs techniques à mesure que le monde numérique évolue, profitant souvent des nouveaux moyens de communications, d'événements dans l'actualité et des nouvelles technologies. La plupart du temps, ils tentent d'inventer des histoires convaincantes pour amener leurs victimes à envoyer de l'argent ou des renseignements de valeur.

Afin de venir en aide à ses entreprises clientes, RBC s'est associée au service de police de Toronto pour cerner les cybermenaces les plus fréquentes chez les petites et moyennes entreprises. Nous espérons que *Le petit livre des grandes fraudes* vous sensibilisera davantage à ces cybermenaces et vous aidera à déjouer les escroqueries qui ciblent actuellement les entreprises comme la vôtre. Vous y trouverez des pratiques exemplaires et des mesures simples à prendre pour protéger votre entreprise, vos employés et vous-même.

RBC a à cœur la cybersécurité de ses clients et de leurs entreprises.

Consultez rbc.com/cyberfute/entreprise pour découvrir d'autres façons d'assurer votre sécurité en ligne !

Au cours de ma carrière, j'ai été témoin des effets dévastateurs du cybercrime sur les gens et sur les entreprises. En effet, les cybercriminels ne se contentent pas de voler des renseignements ou d'autres biens : ils prennent le contrôle de votre vie personnelle ou professionnelle. De plus, tenter de corriger la situation peut demander beaucoup d'énergie et d'argent. Nous savons notamment que les petites entreprises peinent à gérer les cybercrimes. Voilà pourquoi le service de police de Toronto s'associe à la Banque Royale du Canada pour vous tenir informés. En matière de cybercrime, la sensibilisation est la clé pour vous empêcher de devenir une victime.

Le cybercrime est un problème grandissant pour les petites et moyennes entreprises. En 2017, plus du cinquième des entreprises canadiennes a été touché par des incidents de cybersécurité qui ont entravé leurs activités. Hélas, seulement 19 % de ces entreprises ont fait un signalement à un service de police. Sachez que vous n'êtes pas seul. Nous pouvons vous aider à assurer votre protection.

5 mesures à prendre

pour assurer la cybersécurité de votre entreprise

Renforcez la cybersécurité de votre entreprise en adoptant cinq pratiques exemplaires toutes simples.

1. Sauvegarder régulièrement vos données hors site.

Les entreprises possèdent des renseignements de grande valeur pour les cybercriminels : dossiers d'employés et de clients, renseignements financiers, etc. Sauvegardez constamment vos données pour minimiser les conséquences en cas d'attaque par un rançongiciel. Idéalement, les fichiers devraient être sauvegardés dans un système hors site sécuritaire qui crée continuellement de nouvelles versions de toutes les données de l'entreprise.

2. Mettre en œuvre des politiques de sécurité officielles.

Il est essentiel d'établir et d'appliquer des politiques et des pratiques en matière de sécurité pour protéger vos systèmes. Tout le monde doit se soucier de la protection du réseau de l'entreprise. En effet, il ne faut pas oublier que chaque utilisateur est une cible potentielle pour les criminels. Expliquez les politiques et des pratiques en matière de sécurité aux employés afin qu'ils comprennent pourquoi elles sont en place, comment elles s'appliquent et quels sont les risques potentiels pour eux ou pour l'entreprise si elles ne sont pas respectées.

3. Tenir vos logiciels à jour.

Les fabricants de logiciels et d'appareils informatiques déploient périodiquement des mises à jour et des correctifs de sécurité. Les pirates informatiques, les programmes malveillants ou les virus trouvent des failles dans les logiciels (appelées vulnérabilités) et s'en servent pour s'introduire dans vos ordinateurs, téléphones ou tablettes. En installant les mises à jour, vous corrigez ces vulnérabilités et favorisez la sécurité de vos appareils. Pour une sécurité optimale, toute petite entreprise doit fréquemment télécharger et installer chaque mise à jour et correctif sur l'ensemble de ses appareils.

4. Établir un plan d'intervention en cas d'incident.

Un plan d'intervention en cas d'incident contient des instructions et des procédures pour détecter les cyber-incidents, les traiter et en atténuer les effets. Le plan doit nommer les personnes chargées de traiter les incidents, en plus de contenir les coordonnées des partenaires externes, des parties prenantes et des autorités de réglementation. Chaque trimestre, passez le plan en revue et apportez les mises à jour requises.

5. Informer vos employés.

Sensibilisez vos employés aux cybermenaces et aux stratégies utilisées par les cybercriminels pour infiltrer vos systèmes. Montrez-leur comment protéger les données de l'entreprise : apprenez-leur à déceler les indices d'une violation et à utiliser votre réseau de manière sécuritaire. En comprenant les menaces latentes, vos employés peuvent aider à les stopper.


FACTURE
$
$
$

Fausses factures

Ciblant souvent les petites et moyennes entreprises, les OSBL, les municipalités et d'autres petites organisations, les fausses factures incitent les victimes à rediriger des paiements vers un compte frauduleux.

Un employé reçoit un courriel d'une entreprise avec laquelle il fait affaire. Souvent, le message explique qu'une facture est en retard et doit être payée immédiatement sans quoi des intérêts élevés seront imputés. Le courriel peut aussi prétendre que l'entreprise a récemment changé de banque et demander le transfert des paiements dans un « nouveau » numéro de compte.

À première vue, bon nombre de ces « factures » semblent légitimes. Toutefois, elles peuvent comprendre des menaces ou des termes juridiques compliqués qui créent un faux sentiment d'urgence et poussent les destinataires à payer rapidement.

Pour protéger votre entreprise, assurez-vous que les employés chargés du traitement des factures prennent toujours ces mesures :

- **Confirmer** toute nouvelle instruction de paiement reçue par courriel, même à l'interne.
- Dans la mesure du possible, appeler directement la personne qui demande le transfert afin de lui **parler de vive voix**.
- **Communiquer** directement avec le fournisseur ou le client pour confirmer la demande et s'assurer que les changements apportés à la méthode de paiement sont légitimes.
- **Examiner attentivement** chaque paiement avant de l'envoyer, puis s'assurer que toute la correspondance est validée et documentée de façon uniforme au sein de l'entreprise.

Intégrer ces mesures de sécurité toutes simples au processus de paiement peut grandement aider à prévenir les fraudes.

Protégez votre entreprise

SOYEZ VIGILANT
Les employés chargés du traitement des paiements doivent rester vigilants et porter attention à tout changement dans les instructions de paiement. Si vous doutez qu'un fournisseur ait réellement changé ses renseignements bancaires, appelez-le directement pour obtenir une confirmation de vive voix.

SOYEZ PRUDENT
Examinez attentivement chaque facture. N'effectuez aucun paiement si vous n'êtes pas certain que les articles facturés ont bien été commandés et livrés. Dites à vos employés de faire de même.

SOYEZ MÉFIANT
N'oubliez pas que les fraudeurs peuvent facilement créer de faux sites Web ou des adresses courriel qui ont l'air tout à fait légitimes. Pensez-y bien avant de cliquer.

SOYEZ PROACTIF
Avant de faire affaire avec une nouvelle entreprise, recherchez son nom sur Internet avec les termes « fraude » ou « plainte ». Lisez les commentaires à propos de cette entreprise.

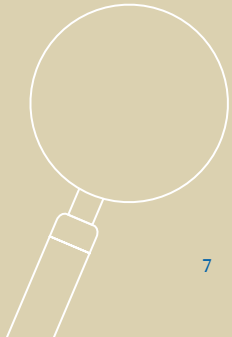
Décelez les indices !

Suscite un sentiment d'urgence. Si un particulier ou une institution financière vous envoie un courriel non sollicité présentant une situation urgente à régler immédiatement, méfiez-vous.

Imite une personne ou un fournisseur de confiance. Pour avoir l'air crédibles, les cybercriminels peuvent prétendre travailler pour l'un de vos partenaires commerciaux.

Contient des pièces jointes et des liens malveillants. Évitez d'ouvrir les liens ou les pièces jointes, car ils peuvent déceler des virus ou des logiciels espions.

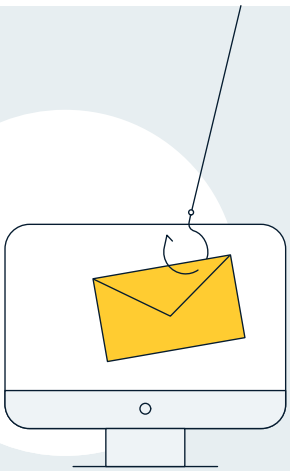
Signalez toute demande suspecte !
Allez aux pages 16 et 17 pour en savoir plus.



Escroqueries courriel du cadre dirigeant

Les escroqueries par courriel existent depuis la naissance d'Internet. Cependant, les techniques ont évolué. Les cybercriminels s'attaquent aujourd'hui à des personnes précises. Ils peuvent notamment se faire passer pour un cadre supérieur (comme le chef de la direction ou le chef des finances) afin de convaincre la victime de mordre à l'hameçon.

Bien qu'il existe de nombreuses escroqueries se rapportant aux cadres supérieurs, deux sont plus fréquentes au sein des petites et moyennes entreprises : les courriels d'affaires compromis et le harponnage.



Courriel d'affaires compromis

Selon le Centre antifraude du Canada (CAFC), les courriels d'affaires compromis ont permis de soutirer plus de cinq milliards de dollars à des entreprises du monde entier, y compris au Canada.

On parle de courriel d'affaires compromis lorsqu'un criminel se fait passer pour un cadre supérieur d'une entreprise, soit en accédant à son compte de courriel d'entreprise ou en créant un faux compte. Grâce à des tactiques de piratage psychologique et de recherche, souvent dans les médias sociaux, le criminel rédige des courriels crédibles et les envoie à un employé qui semble être autorisé à virer des fonds. Il espère ainsi l'amener à transférer de l'argent dans un faux compte.

Harponnage

Le harponnage est une escroquerie de mystification ciblant une entreprise ou un employé au moyen de courriels personnalisés. Cette machination vise à obtenir un accès non autorisé à des données sensibles, à des fonds ou à des systèmes informatiques.

Les criminels utilisent notamment les médias sociaux pour recueillir des renseignements sur leurs cibles (adresses courriel, titres de poste, champs d'intérêt, etc.) et créer de faux courriels très convaincants.

Protégez votre entreprise

SOYEZ VIGILANT
Renseignez vos employés sur ces types d'escroquerie et demandez-leur de se méfier des demandes urgentes ou suspectes envoyées par courriel.

SOYEZ PRUDENT
Faites attention à ce que vous divulguez sur les médias sociaux. Les criminels peuvent utiliser les renseignements partagés sur ces sites, de même que sur votre propre site Web, pour frauder votre entreprise.

SOYEZ MÉFIANT
Assurez-vous de toujours lire les détails de la commande, confirmer la validité du client et vérifier les renseignements de la facture avant de transférer des fonds.

SOYEZ PROACTIF
N'effectuez pas de virements de fonds par courriel. Mettez en œuvre un autre processus de communication en personne ou par téléphone permettant de vérifier la légitimité des demandes.

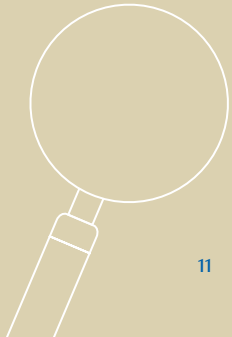
Décelez les indices !

Le courriel semble provenir d'un cadre supérieur, comme le chef de la direction ou le chef des finances.

La demande paraît urgente et hautement confidentielle.
On demande souvent aux destinataires ciblés d'ouvrir une pièce jointe malveillante ou de cliquer sur un lien menant à un faux site Web où ils devront saisir leur mot de passe, numéro de compte et code d'accès.

Adresses courriel d'apparence authentique. Les criminels enregistrent des noms de domaine ressemblant à ceux des entreprises ciblées, par exemple @votreentreprise1.com plutôt que @votreentreprise.com. Ensuite, les fraudeurs n'ont qu'à rechercher et à apposer les noms de vrais cadres avec le faux nom de domaine pour créer des courriels encore plus convaincants.

Signalez toute demande suspecte !
Allez aux pages 16 et 17 pour en savoir plus.



Extorsions en ligne

Selon Statistique Canada, en 2017, environ 40 % des cyberattaques ciblant des entreprises se sont traduites par une tentative de vol ou une demande de rançon[1].

L'extorsion en ligne consiste à intimider une personne ou une entreprise afin qu'elle paie une « rançon » pour récupérer des biens numériques volés. Ces biens peuvent être des documents ou des fichiers de base de données contenant des renseignements confidentiels sur la victime, les activités d'une entreprise ou ses intérêts financiers.

L'extorsion en ligne peut prendre différentes formes : rançongiciel, chantage en ligne et même hameçonnage. Nous pouvons tous être victimes d'une extorsion en ligne.

[1] Les statistiques ci-dessus sont tirées de l'Enquête canadienne sur la cybersécurité et le cybercrime de 2017.

Chantage en ligne

La plupart du temps, la victime reçoit un courriel la menaçant de diffuser des photos ou des vidéos explicites qui pourrait ternir sa réputation. On lui demande alors d'envoyer de l'argent ou de se plier aux demandes des criminels.

L'expéditeur du courriel peut aussi prétendre avoir enregistré du matériel explicite après avoir pris le contrôle de votre écran et de votre caméra Web. En vous embarrassant et en vous faisant peur, le criminel cherche à vous faire payer sans réfléchir.

Rançongiciel

En 2016 et en 2017, les attaques de rançongiciel ont permis de voler 5,7 millions de dollars aux petites et moyennes entreprises canadiennes[2].

Un rançongiciel est une forme de logiciel malveillant (maliciel) permettant à des cybercriminels de verrouiller à distance des fichiers sur votre ordinateur ou votre appareil mobile. Les criminels vous proposeront alors de restaurer l'accès à vos fichiers en échange d'une certaine somme.

Un rançongiciel peut s'infiltrer dans un ordinateur de plusieurs façons, mais l'infection se fait habituellement lorsqu'une personne clique sur une pièce jointe ou un lien malveillant dans un courriel hameçon. Une fois l'appareil infecté, une note de « rançon » s'affiche à l'écran. Celle-ci vise souvent à effrayer ou à extorquer de l'argent aux victimes.

[2] Rapport de Datto sur l'état des escroqueries par rançongiciel au Canada

Protégez votre entreprise

SOYEZ VIGILANT
Investissez dans des systèmes de sécurité protégeant les réseaux, ordinateurs et appareils mobiles de votre entreprise. Mettez à jour votre logiciel de sécurité, changez vos mots de passe et sauvegardez fréquemment vos données. Conservez les sauvegardes dans un système hors site et hors ligne.

SOYEZ PRUDENT
N'ouvrez aucun courriel, pièce jointe ou lien non sollicité ou de source inconnue.

SOYEZ MÉFIANT
Si vous recevez un courriel menaçant, ne paniquez pas, ne répondez pas et n'envoyez surtout pas d'argent. Signalez le courriel hameçon et alertez les autorités locales.

SOYEZ PROACTIF
Assurez-vous que vos comptes en ligne sont protégés par des mots de passe uniques et sécuritaires. Si possible, activez l'authentification à deux facteurs. Si vous croyez que votre compte est compromis ou que votre mot de passe a été découvert, changez-le immédiatement.

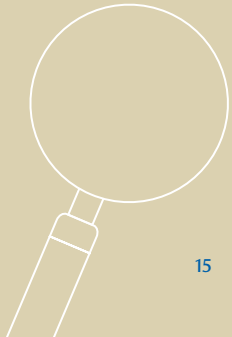
Décelez les indices !

Le message est menaçant et suscite la peur et la panique. Par exemple, vous pouvez recevoir un courriel révélant votre mot de passe et prétendant qu'un cybercriminel s'est introduit dans votre ordinateur.

Vous avez alors un court délai, normalement entre 24 et 72 heures, pour payer avant que la « clé privée » soit détruite et vos fichiers, perdus à jamais.

La rançon demandée s'élève généralement à quelques centaines de dollars et le transfert doit se faire par Bitcoin, UKash, Green Dog ou tout autre système de paiement numérique.

Signalez toute demande suspecte !
Allez aux pages 16 et 17 pour en savoir plus.



Signaler une cyberfraude à RBC

RBC ne vous demandera jamais de vérifier des renseignements personnels ou financiers par courriel, par texto ou au téléphone.

Communiquez immédiatement avec RBC si vous croyez que votre identité ou vos renseignements personnels ont été volés, ou bien que vos comptes sont compromis. Notre équipe d'experts dévoués vous indiquera les mesures appropriées à prendre.

Centre de soutien clientèle, Services bancaires en ligne RBC Express®
1 800 769-2535

Infoligne entreprise (jour et nuit)
1 888 830-9751

Services bancaires par téléphone
1 800 769-2511

Banque en direct/ Services bancaires mobiles
1 800 769-2555

Cartes de crédit
1 800 769-2512

RBC Bank (Georgia), N.A.
1 800 769-2553

ATS/Téléimprimeur
1 800 661-1275

Fraude par courriel et faux sites Web

Si vous croyez que vos renseignements confidentiels ont été volés ou obtenus par un fraudeur, que ce soit en ligne, par téléphone ou par tout autre moyen, appelez-nous aussitôt.

Si vous recevez un courriel hameçon, informez-nous en faisant suivre le message suspect à l'adresse **phishing@rbc.com** aux fins d'analyse. Veuillez noter que l'adresse **phishing@rbc.com** est liée à une boîte aux lettres automatisée réservée au signalement des courriels hameçons et des sites Web frauduleux. Nous ne pouvons répondre aux courriels qui y sont envoyés. Si vous avez une question, veuillez composer l'un des numéros de téléphone ci-dessus pour parler à un représentant.

Pour signaler un faux site Web utilisant le nom d'une entreprise de RBC, écrivez à l'adresse **phishing@rbc.com.** Inscrivez « Faux site Web RBC » dans l'objet du courriel. N'oubliez pas de coller l'URL (adresse Web) complète dans le corps de votre message. Vous trouverez des trucs pour déceler les courriels hameçons et les faux sites Web au **rbc.com/cyberfute.**

Restez à l'affût des dernières cyberfraudes visant les clients de RBC.
Pour en savoir plus, allez au rbc.com/cyberfute/alertes.

Signalement – Conseil du service de police de Toronto

La majorité des entreprises canadiennes ne signalent pas les incidents de cybersécurité aux autorités. Toutefois, le service de police de Toronto recommande de communiquer avec les autorités locales pour signaler toute fraude ou escroquerie. En effet, chaque signalement compte et aide grandement les enquêteurs. Assurez-vous d'obtenir un numéro de rapport aux fins de référence.

Communiquez avec les organismes suivants selon le cas :

Pour signaler un cyberincident ou une fraude, communiquez avec le Centre antifraude du Canada (CAFC) au 1 888 495-8501 ou au www.antifraudcentre.ca.

Vous pouvez aussi facilement signaler un incident en ligne dans le nouveau Système de signalement des fraudes (SSF).

Les infrastructures essentielles, les entreprises, ainsi que les gouvernements provinciaux, territoriaux et municipaux doivent signaler immédiatement tout incident au Centre canadien de réponse aux incidents cybernétique (CCRIC) par courriel ps.cyberincident.sp@canada.ca.

Le CCIRC aidera à atténuer et à prévenir les effets.

En cas de vol d'identité (LPRPDE), communiquez avec le commissaire à la protection de la vie privée du Canada au 1 800 282-1376 ou au www.priv.gc.ca/fr pour obtenir de l'aide et des conseils.

La Loi sur la protection des renseignements personnels et les documents électroniques exige de signaler au Commissariat à la protection de la vie privée toute atteinte aux mesures de sécurité touchant des renseignements personnels.

Nota : D'autres lois sur la protection des renseignements personnels semblables à la LPRPDE sont en vigueur au Québec, en Colombie-Britannique et en Alberta. Les habitants de ces provinces doivent communiquer avec leur commissaire provincial.

Si l'une de vos pièces d'identité délivrée par le gouvernement fédéral (NAS, passeport, etc.) est compromise, appelez Service Canada au 1 800 O-Canada.

Si vous croyez que votre permis de conduire ou votre carte d'assurance maladie est compromis, communiquez avec le ministère du Transport ou de la Santé de votre province ou territoire.

Associations sectorielles de cybersécurité

Les associations sectorielles de cybersécurité peuvent vous fournir des renseignements plus détaillés et des conseils sur la cybersécurité des petites et moyennes entreprises. Si vous avez besoin d'une aide externe, elles peuvent également vous recommander des fournisseurs de services dans votre région.

Échange canadien de menaces cybernétiques
https://cctx.ca/membership/

Association des professionnels de la vérification et du contrôle des systèmes d'information (ISACA)
www.isaca.org/membership/Pages/default.aspx

Information Systems Security Certification Consortium, Inc. (ISC2)
www.isc2.org/chapters/Default.aspx

Information Systems Security Association (ISSA)
www.issa.org/?page=ChaptersContact

Soyez cyberfuté RBC®

⚠ Souvenez-vous !

Un plan de prévention, d'intervention ou de reprise peut aider à vous préparer en vue d'un cyberincident. D'ailleurs, vous trouverez la Grille de gestion de crise en cybersécurité sur le site Web de RBC.

Pour en savoir plus, allez à

rbc.com/cyberfute/entreprise

VPS106325

124145 (12/2019)