Sécurité numérique et escroqueries : Entreprises

Comment protéger votre entreprise, vos données et vos résultats financiers dans un monde connecté

Table des matières

L’importance de la cybersécurité

Dans l’économie axée sur le numérique d’aujourd’hui, les entreprises de toutes tailles comptent sur Internet pour servir leurs clients, gérer leurs activités et assurer leur croissance. Toutefois, cette connectivité comporte des risques, en particulier pour les petites entreprises, qui peuvent ne pas disposer des mêmes ressources que les grandes organisations pour se protéger contre les escroqueries et les cybermenaces.

La bonne nouvelle, c’est que vous n’avez pas à être un expert en technologie pour agir. Ce guide présente des pratiques essentielles en matière de cyberhygiène, la façon de repérer les escroqueries qui ciblent les entreprises et les mesures à prendre si votre entreprise est touchée par une fraude ou un cyberincident.

Connaître les fondements de la cybersécurité : Liste de vérification pour protéger votre entreprise

L'adoption de solides habitudes en matière de cybersécurité peut vous aider à protéger vos systèmes, vos données, vos clients et votre réputation. Ces mesures proactives sont essentielles pour réduire les risques.

☐ **Installez des outils de sécurité dans vos systèmes et tenez vos systèmes et logiciels à jour**

Les bons outils antivirus et antilogiciels malveillants peuvent contribuer à vous protéger contre les attaques malveillantes. L'application régulière des mises à jour et des correctifs permet de combler les failles de sécurité et d'améliorer la résilience du système.

☐ **Installez un pare-feu de système de noms par domaine (DNS)**

Les logiciels pare-feu peuvent protéger votre réseau d'entreprise contre le trafic Internet malveillant en analysant le trafic du réseau et en empêchant tout trafic indésirable d'atteindre votre réseau. Le site Web Pensez cybersécurité du gouvernement du Canada explique comment les pare-feu apportent une couche de protection supplémentaire à vos appareils.

☐ **Créez des mots de passe et des phrases d'identification sûrs et uniques, et assurez-vous que vos employés font de même**

Le fait d'exiger des justificatifs d'ouverture de session pour tous les employés et comptes peut empêcher les accès non autorisés. Mettez régulièrement à jour vos mots de passe et ne communiquez jamais vos justificatifs d'accès à d'autres personnes.

☐ **Sauvegardez régulièrement les données**

Songez à utiliser un système de stockage hors site sécuritaire et à conserver des sauvegardes infonuagiques et physiques. Vous pourrez ainsi récupérer l'information sensible si votre entreprise est la cible d'une attaque par logiciel de rançon ou logiciel malveillant.

☐ **Utilisez un VPN pour l'accès à distance**

Les réseaux privés virtuels (VPN) chiffrent les données et sécurisent l'accès des employés à votre réseau d'entreprise.

☐ **Limitez le transfert de données et l'accès aux données**

Limitez l'accès des employés selon le poste afin d'ajouter un niveau de contrôle à vos données. Vérifiez régulièrement qui a accès aux systèmes et supprimez les accès des employés qui quittent leur poste ou qui changent de rôle. Désactivez également les fonctions de partage de fichiers pour réduire les risques.

☐ **Sensibilisez vos employés**

En matière de cybersécurité, les employés sont souvent le maillon faible des entreprises. Offrez une formation continue et pratique à la cybersécurité afin qu'ils puissent reconnaître les escroqueries et y réagir de façon appropriée.

☐ **Dotez votre entreprise de politiques de cybersécurité formelles**

L'établissement de directives claires aide les employés à comprendre leurs responsabilités et à savoir quoi faire en cas de crise.

Repérer les escroqueries courantes

Les entreprises sont des cibles attrayantes pour les escrocs, car elles gèrent de précieuses données, traitent des opérations importantes et comptent de nombreux employés – chacun pouvant être un point d'entrée pour la fraude. Si elle sait reconnaître les signaux d'alerte, votre équipe sera mieux en mesure d'éviter de graves conséquences financières et opérationnelles.

Escroqueries par piratage psychologique

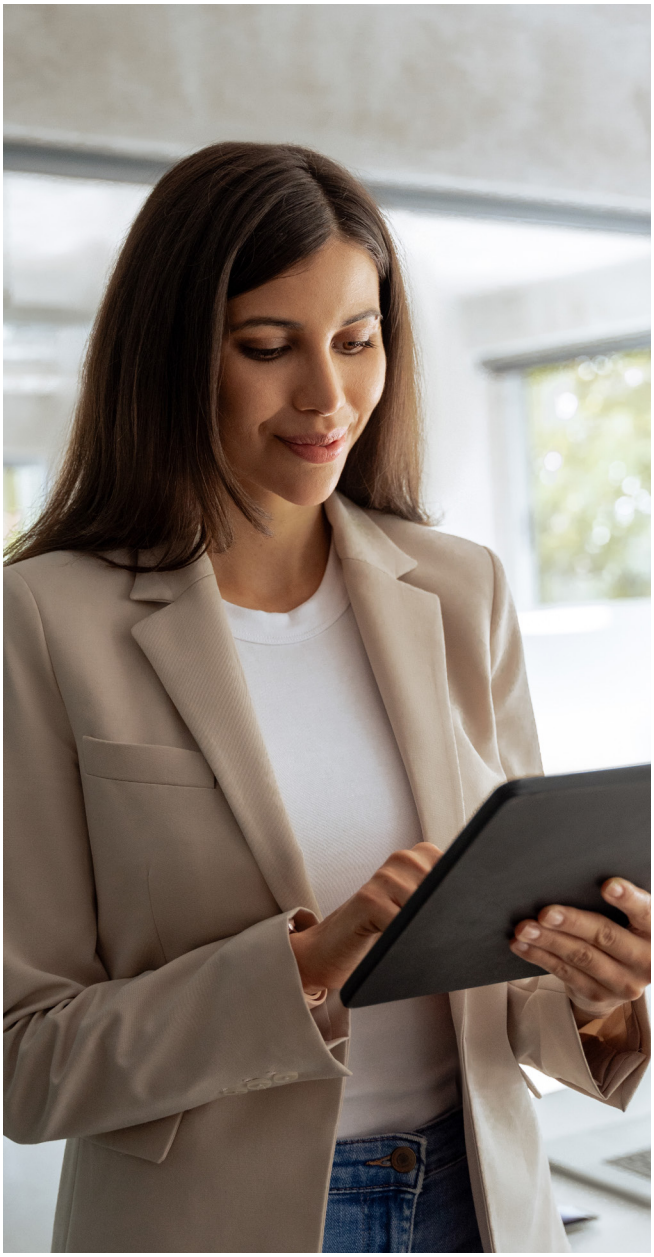
L'escroquerie par piratage psychologique cible le côté humain de votre entreprise, c'est-à-dire vos employés. Dans ce type d'escroquerie, les escrocs manipulent le personnel pour l'inciter à communiquer des renseignements confidentiels ou à effectuer une action non autorisée, souvent en se faisant passer pour un collègue, un fournisseur ou un client en situation d'urgence.

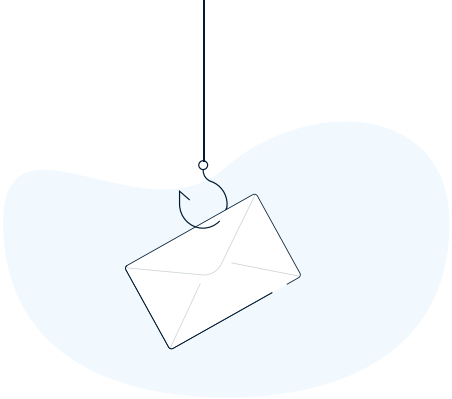
Pour prévenir ces attaques, il est essentiel que vous appreniez à votre équipe à prendre un moment pour vérifier les demandes inhabituelles et à suivre les procédures de recours hiérarchique en vigueur.

Escroqueries par courriel (hameçonnage)

Les courriels hameçons semblent souvent provenir de sources légitimes, comme des fournisseurs ou des dirigeants d'entreprise. Il s'agit généralement d'une demande urgente de cliquer sur un lien ou de télécharger une pièce jointe dans le but d'installer un logiciel malveillant ou d'accéder à des renseignements confidentiels.

Bien que ces escroqueries soient de plus en plus sophistiquées, il existe des moyens de les repérer : de petites incohérences dans l'adresse, la langue ou l'URL de l'expéditeur peuvent aider votre équipe à détecter un faux courriel.





Logiciel de rançon

Le logiciel de rançon est l'une des cybermenaces les plus dommageables pour les entreprises. Il chiffre vos données et exige un paiement pour les déverrouiller. Les attaques commencent souvent par un courriel hameçon ou un fichier infecté. Gardez à l'esprit que même si vous payez la rançon, rien ne garantit que l'escroc déchiffrera vos fichiers ou ne vendra pas les données en ligne.

Des sauvegardes régulières, l'utilisation de logiciels de sécurité et la formation des employés sont votre meilleure ligne de défense – et peuvent réduire les temps d'arrêt en cas de problème.

Escroqueries par usurpation d'identité bancaire

Ces escroqueries commencent souvent par un appel, un texto ou un courriel prétendant provenir de votre banque. Les fraudeurs peuvent contacter votre personnel au sujet d'une brèche de sécurité ou d'un problème lié à un compte, puis lui demander des justificatifs d'ouverture de session, des codes d'authentification ponctuels ou même des virements de fonds pour corriger la situation.

Ces interactions peuvent sembler tout à fait légitimes et ont réussi à tromper des employés, surtout ceux peu formés à la cybersécurité.

Il convient de rappeler à votre équipe que la meilleure chose à faire en cas de doute est de raccrocher et d'appeler directement la banque en utilisant un numéro connu.

Escroqueries par téléphone (hameçonnage vocal et hameçonnage par texto)

Les escroqueries par téléphone utilisent des appels vocaux ou des textos pour usurper l'identité de fournisseurs, de banques, voire d'organismes gouvernementaux. Ces escroqueries misent souvent sur l'urgence ou la peur pour soutirer des renseignements confidentiels, comme les identifiants de compte ou les approbations de paiement.

N'oubliez pas de rappeler au personnel de vérifier chaque demande de façon indépendante (c.-à-d. en rappelant à un numéro de confiance) avant d'y donner suite.

Escroqueries s'appuyant sur l'IA

L'intelligence artificielle (IA) permet aux fraudeurs de créer des escroqueries plus convaincantes, comme le clonage de voix, la rédaction de courriels impeccables ou la création d'appels vidéo hypertruqués. Partout dans le monde, des entreprises ont été victimes de fausses demandes de fournisseurs, d'escroqueries par usurpation de l'identité d'un chef de la direction et même d'escroqueries par agents virtuels, le tout amélioré par l'IA.

Il est plus important que jamais d'être prudent et de vérifier l'identité de la personne à l'autre bout de la ligne.

Escroqueries par courriel d'affaires compromis ou par courriel d'un fournisseur

L'escroquerie par intrusion dans un courriel d'entreprise est une attaque ciblée dans le cadre de laquelle des fraudeurs détournent ou usurpent des comptes de courriel de confiance, souvent ceux de cadres, de fournisseurs ou de services internes, pour demander des télévirements, modifier des données de paiement ou obtenir des renseignements confidentiels. Ces courriels peuvent sembler tout à fait légitimes et sont souvent programmés pour correspondre à des activités commerciales réelles, comme la conclusion d'une vente ou l'émission d'une facture.

L'escroquerie par courriel d'un fournisseur se produit lorsque le fraudeur envoie une demande qui semble provenir d'un fournisseur existant. Dans bien des cas, le message informe le destinataire d'une modification au compte de paiement ou aux renseignements sur le bénéficiaire au dossier afin de rediriger les fonds dans un compte compromis. Les demandes ont habituellement un caractère urgent et exigent un traitement confidentiel. Elles sont souvent bien formulées, adaptées aux entreprises ciblées et élaborées de façon à ne pas éveiller les soupçons.

Ce qui rend l'escroquerie par intrusion dans un courriel d'entreprise et par courriel d'un fournisseur si dangereuse, c'est qu'elle exploite la confiance et la routine. Un courriel bien rédigé peut échapper à la vigilance même des employés les plus prudents, surtout s'il semble provenir d'une personne en position d'autorité. Les signaux d'alerte courants comprennent les demandes de paiement urgentes, les changements apportés aux directives de paiement ou un langage ou un ton inhabituels.

Les signaux d'alerte courants comprennent les demandes de paiement urgentes, les changements apportés aux directives de paiement ou un langage ou un ton inhabituels.

Escroqueries liées aux placements et à la cryptomonnaie

Les escroqueries liées aux placements et à la cryptomonnaie ciblent souvent des personnes par des moyens sollicités ou non. Les escrocs vous invitent à investir dans des occasions (souvent liées à la cryptomonnaie) en promettant des taux de rendement élevés dans un court laps de temps, avec peu ou pas de risque.

Les escrocs créent de faux sites Web et des publicités et peuvent aussi se faire passer pour des sociétés de confiance ou des personnes connues. Ils utilisent parfois la technologie d'hypertrucage pour se faire passer pour quelqu'un d'autre. Ils adoptent aussi une approche à long terme : ils font de la sollicitation par les plateformes de médias sociaux, des applications de messagerie et même des sites de rencontre, prenant souvent le temps d'établir la confiance. Ils peuvent partager des « saisies d'écran » ou des « graphiques des tendances » en direct pour illustrer l'évolution du placement. Portez attention aux signaux d'alerte tels comme des instructions d'envoi de télévirements à des sociétés de cryptomonnaie, de télévirements ou de dépôts dans des GAB Bitcoin, où l'escroc s'empare ensuite des fonds.

Assurez-vous d'avoir un accès direct à votre compte de placement et de pouvoir vérifier le rendement de façon indépendante. Faites toujours des recherches approfondies avant d'investir, et n'oubliez pas que si une occasion de placement semble trop belle pour être vraie, il s'agit probablement d'une escroquerie.

Prévention, protection et reprise

En matière de cyberincidents, la question n'est pas si votre entreprise sera ciblée, mais quand. Un plan bien défini peut vous aider à protéger votre entreprise contre les escroqueries, à réagir rapidement et à limiter les dégâts.

Les trois étapes de votre plan :

1. Création de procédures préalables

La meilleure façon de gérer un cyberévénement est de s'y préparer avant qu'il se produise. Voici quelques mesures que votre entreprise peut prendre pour se préparer.

☐ **Identifier les principaux acteurs**
Formez une équipe de gestion de crise interfonctionnelle qui comprend les TI, les services juridiques, l'exploitation et les communications.

☐ **Établir des plans d'intervention pour les scénarios probables**
Pensez à des types de cyberévénements, comme les rançongiciels ou les vols de données, et établissez des procédures pour les gérer.

☐ **Élaborer une stratégie de communication claire**
Ayez à portée de main les coordonnées de vos principales parties prenantes, notamment les clients, les partenaires, les organismes de réglementation, les employés et les personnes-ressources clés en matière de technologie (internes ou externes à votre entreprise), comme votre chef de la technologie, votre service des TI et vos fournisseurs de services. Sachez avec qui communiquer et comment le faire, ce qui permettra d'obtenir une réponse plus rapidement et de communiquer de façon transparente.

☐ **Tester régulièrement votre plan**
Votre plan doit évoluer tout autant que les menaces. Réexaminez-le, modifiez-le et testez-le à intervalles réguliers.

2. Établissement de stratégies de prévention

Vos dirigeants et vos employés ont un rôle à jouer pour assurer la sécurité de votre entreprise. Les pratiques suivantes peuvent vous aider à prévenir les escroqueries et les fraudes au sein de votre entreprise.

☐ **Effectuer régulièrement des sauvegardes conservées hors site**
En sauvegardant vos données dans un système sécurisé hors site et en mettant régulièrement à jour ces sauvegardes avec les nouvelles données, vous pourrez restaurer rapidement vos systèmes si jamais vos données sont bloquées par un rançongiciel.

☐ **Donner la priorité aux correctifs**
Mettez à disposition et installez régulièrement des mises à jour sur tous les appareils de votre réseau afin de supprimer les failles de sécurité pouvant être connues des cybercriminels.

☐ **Mettre en œuvre des politiques de sécurité officielles**
En établissant des politiques de sécurité officielles dans l'ensemble de votre entreprise, vos employés n'auront plus à se poser de questions sur la sécurité. Imposez l'utilisation de mots de passe complexes et uniques, utilisez l'authentification multifacteur si possible et limitez l'accès des employés aux seules données nécessaires pour faire leur travail.

☐ **Sensibiliser les employés**
Il suffit qu'un seul employé clique sur un lien ou télécharge un fichier malveillant et cela coûtera très cher à votre entreprise. Formez les employés aux attaques courantes pour qu'ils sachent comment repérer les courriels suspects ou les fichiers dangereux. Assurez-vous également qu'ils savent qui appeler au service des TI s'ils cliquent sur un lien suspect ou si leur ordinateur est attaqué.

☐ **Donner la priorité aux investissements dans les technologies de cybersécurité**
Il existe des milliers de produits de cybersécurité qui peuvent réduire les risques liés aux cyberattaques. Déterminez les points faibles de vos systèmes avec votre équipe du service des TI afin d'investir stratégiquement votre temps, votre argent et vos ressources dans la sécurisation de votre entreprise et la réduction des risques.

3. Mise en place d'un plan d'intervention
Pour beaucoup d'entreprises, la tendance naturelle est de garder le silence concernant une attaque afin d'éviter toute publicité négative. En effet, seulement 9,6 % des entreprises déclarent les incidents à la police*. Cependant, cela vous empêche d'obtenir le soutien dont vous avez besoin pour y répondre efficacement tout en permettant aux criminels de s'attaquer à la prochaine victime.

La section suivante indique qui joindre en cas de cyberattaque. Assurez-vous d'avoir les renseignements nécessaires à portée de main afin de pouvoir agir rapidement et de réduire au minimum les dégâts.

Signalement et réponse : ressources à contacter

Le signalement rapide d'une fraude peut limiter l'incidence sur votre entreprise et contribuer à prévenir des attaques semblables envers d'autres entreprises. Voici les mesures à prendre si votre entreprise est victime d'une escroquerie ou d'un cyberincident.

1. Avisez votre banque

Si votre entreprise est victime de fraude, votre banque peut vous aider à protéger vos comptes et à empêcher d'autres pertes. Communiquez avec votre banque sans tarder pour que toutes les cartes de crédit d'entreprise ou tous les comptes touchés puissent être bloqués, surveillés et remplacés rapidement. La banque dispose de spécialistes de la lutte antifraude prêts à vous guider et à assurer la sécurité de vos informations.

Clients de RBC

Si vous êtes un client de RBC et que vous avez été victime de fraude, communiquez sans délai avec votre succursale, votre bureau local, ou appelez-nous. 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)
- RBC Bank (Georgia), N.A. : 1 800 769-2553
- ATS/Téléimprimeur : 1 800 661-1275

Si votre entreprise est située aux États-Unis, veuillez également aviser les autorités locales et la FTC (Federal Trade Commission) en composant le 1 877 438-4338.

2. Alertez les agences d'évaluation du crédit

Si un fraudeur a accédé aux systèmes de votre entreprise, prévenez immédiatement les agences d'évaluation du crédit. Elles peuvent ajouter une alerte à la fraude à votre dossier afin de limiter l'ouverture de comptes non autorisés au nom de votre entreprise. Il est également judicieux de consulter votre rapport de solvabilité pour détecter toute activité douteuse.

Les deux principales agences d'évaluation du crédit sont Equifax et TransUnion. Il est préférable de contacter les deux, car elles travaillent indépendamment.

Canada :

TransUnion
1 877 525-3823
transunion.ca

Equifax
1 877 323-2598
equifax.ca

États-Unis :

TransUnion
1 800 888-4213
transunion.com

Equifax
1 800 685-1111
equifax.com

Experian
1 888 397-3742
experian.com

International (îles Britanniques) :

Experian
+44 844 481-8000
Appel depuis l'étranger (hors Royaume-Uni)

0844 481-8000
Appel local (au Royaume-Uni)
experian.co.uk

Equifax
equifax.co.uk
(tous les contacts se font en ligne, sauf si vous êtes membre du service Equifax)

3. Communiquez avec les autorités chargées de l'application des lois et les agences de lutte contre la fraude

En signalant une cyberattaque aux autorités, vous vous assurez d'obtenir le soutien dont votre entreprise a besoin pour réagir, tout en les aidant à mener leurs enquêtes criminelles.

Autorités chargées de l'application des lois
Les autorités locales ou fédérales disposent de spécialistes qui peuvent aider à intervenir rapidement et à coordonner l'aide avec d'autres services gouvernementaux. Elles réuniront également les preuves essentielles pour mener une enquête criminelle afin que les pirates puissent être traduits en justice.

Centre antifraude du Canada (CAFC)
Le Centre antifraude du Canada (CAFC) est un service de police national qui recueille de l'information sur la fraude dans l'ensemble du Canada et aide les services de police compétents dans leurs efforts d'application de la loi et de prévention de la fraude. Signalez tout incident en ligne à l'adresse reportcyberandfraud.canada.ca ou téléphonez sans frais au 1 888 495-8501.

Centre canadien pour la cybersécurité
Le Centre canadien pour la cybersécurité travaille avec les autorités chargées de l'application des lois, les entreprises et le secteur public pour diriger la réponse du gouvernement aux événements liés à la cybersécurité. Envoyez un courriel à l'adresse contact@cyber.gc.ca ou téléphonez sans frais au 1-833-CYBER-88 (1 833 292-3788).

Si vous faites des affaires à l'extérieur du Canada, communiquez avec les organismes suivants :

États-Unis :
• Federal Trade Commission (FTC) : reportfraud.ftc.gov
• FBI Internet Crime Complaint Center (IC3) : ic3.gov

Royaume-Uni :
• Action Fraud (le centre de signalement national du Royaume-Uni) : actionfraud.police.uk

Les cybermenaces sont une réalité pour les entreprises de tous types et de toutes tailles. Cependant, avec les bonnes procédures, les bons outils et une bonne sensibilisation, elles n'ont pas à se transformer en situation de crise immédiate. En mettant en place des mesures de protection rigoureuses, en formant votre équipe et en vous préparant aux imprévus, vous pouvez réduire vos risques et réagir en toute confiance en cas d'incident.

La cybersécurité n'est pas seulement un enjeu de TI, c'est un impératif commercial. Plus votre équipe est préparée, plus il est difficile pour les escrocs de causer des dommages ou des perturbations.

Remarques

Liste de verification

- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐
- ☐

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

Sources : Sécurité publique Canada, Profil des entreprises canadiennes qui signalent les cybercrimes à la police.

Créé en : octobre 2025
Dernière mise à jour : decembre 2025