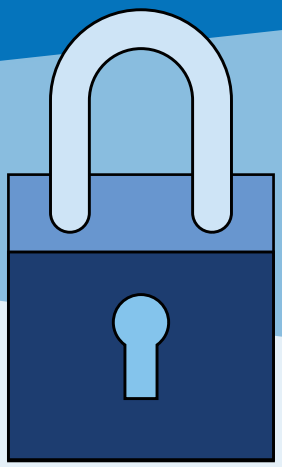
Trousse de prévention de la fraude pour petites et moyennes entreprises

Protégez votre entreprise des cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

Version 2026

Une trousse préparée par l'Association des banquiers canadiens en vue d'aider les propriétaires et les gestionnaires de PME à comprendre les menaces à leur cybersécurité et à adopter des mesures efficaces pour se protéger et protéger leurs employés de la fraude et du cybercrime.

Les banques au Canada ne ménagent aucun effort pour détecter et éviter les cybermenaces. Elles collaborent étroitement entre elles, ainsi qu'avec les organismes de réglementation, les forces de l'ordre et tous les niveaux de gouvernement afin de protéger leurs clients, de même que le système financier dans son ensemble, contre le crime financier. En tant que propriétaire ou gestionnaire d'une petite entreprise, vous pourrez adopter de simples mesures vous permettant de déceler les arnaques les plus fréquentes et de vous protéger, ainsi que vos employés, de la fraude financière.

Contenu

01 Fondements de la cybersécurité

02 Liste de vérification de la cyberhygiène

03 Survol des arnaques les plus fréquentes

- 03.1 Hameçonnage et fraude par courriel
- 03.2 Rançongiciels
- 03.3 Usurpation de l'identité de dirigeants
- 03.4 Fraude du courriel d'entreprise compromis
- 03.5 Arnaques du code à usage unique
- 03.6 Arnaques vocales

04 Protection des données personnelles des clients

05 Conseils pour vos employés

06 Comment signaler une fraude

07 Ressources additionnelles

Fondements de la cybersécurité

pour petites entreprises

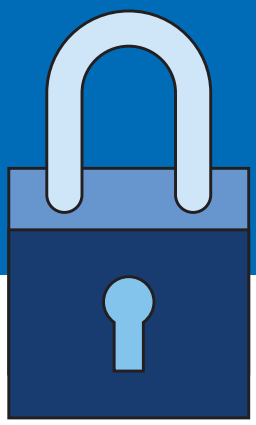
La prépondérance du numérique dans l'économie d'aujourd'hui signifie que les entreprises, petites ou grandes, utilisent Internet pour gérer leurs opérations, servir leurs clients et poursuivre leur croissance.

Les cybercriminels visent les petites entreprises vu qu'elles n'auraient pas nécessairement les moyens de mettre en place de solides mesures de sécurité. En tant que propriétaire d'une petite entreprise, vous devez être toujours conscient des mesures de cybersécurité afin de réduire les risques, surtout qu'il n'est pas nécessaire d'être un expert en informatique pour adopter des pratiques de cyberhygiène efficaces.

Que doit comporter un plan de cybersécurité?

Un plan de cybersécurité doit inclure :

- Des procédures de protection pour les données, les ordinateurs et les réseaux de l'entreprise contre les cyberattaques.
- La formation obligatoire des employés sur les principes de sécurité et la détection des escroqueries qui visent particulièrement les petites entreprises.
- Des processus de réaction aux menaces à la cybersécurité et un plan pour mettre à jour et calibrer les mesures de sécurité selon les changements dans les vulnérabilités de l'entreprise.



Qu'est-ce que la cybersécurité?

La cybersécurité est un ensemble de procédures établies dans l'objectif de protéger les réseaux, les systèmes, les employés et les données de votre petite entreprise contre les cybermenaces. Les cybercriminels visent les petites entreprises afin de récolter des données utilisables pour lancer des attaques dont l'objectif est de voler des renseignements ou de l'argent propres à l'entreprise ou à ses clients.

Liste de vérification de la cyberhygiène

Protection des données, des ordinateurs et des réseaux de votre entreprise contre les cyberattaques

Pour que le risque de cybermenaces envers votre entreprise diminue, votre plan de cybersécurité devra inclure ces cinq étapes.

1. Installation des outils de sécurité adéquats

Installez un antivirus, un antimaliciel et un pare-feu sur tous les réseaux et les appareils connectés de votre entreprise. Ces programmes doivent être régulièrement activés et maintenus à jour pour veiller à la protection de vos données contre les maliciels.

2. Création de mots et de phrases de passe distincts et complexes

Utilisez des mots (ou phrases) de passe distincts et complexes pour tous vos comptes et vos services Internet. Incitez vos employés à faire de même. Vous trouvez des conseils sur la création de phrases de passe sur le site de l'ABC : cba.ca/article/piratage-dix-des-pires-mots-de-passe

Imposez l'utilisation de l'authentification multifactorielle (AMF) sur les appareils et les comptes de l'entreprise. L'AMF offre un niveau de sécurité complémentaire au mot (ou phrase) de passe. Ainsi, l'accès à l'appareil ou au compte ne sera accordé qu'aux personnes autorisées.

3. Mises à jour des systèmes d'exploitation et des applications

Utilisez la version la plus récente du système d'exploitation de vos ordinateurs et de vos appareils connectés. Chaque nouvelle version comporte d'importants correctifs de sécurité pour vous faire éviter les failles connues. L'automatisation des mises à jour du système d'exploitation, des applications et des périphériques veillera à l'installation des importants correctifs de sécurité qui vous protègeront des récentes menaces.

4. Programmation des sauvegardes régulières des données

Sauvegardez fréquemment vos fichiers sur des plateformes externes. De plus, instaurez des procédures claires pour récupérer les fichiers ainsi sauvegardés et prévoyez une liste de vérification de ces sauvegardes régulières. Le guide Pensez cybersécurité pour les petites et moyennes entreprises, conçu par le gouvernement du Canada, présente à la section 7.1 plusieurs options de sauvegarde et de restauration pour les données et les fichiers de l'entreprise.

Liste de vérification de la cyberhygiène (Suite)

5. Lignes directrices sur le partage et le téléchargement de données dans votre entreprise

Définissez des lignes directrices internes claires quant au contenu qui peut ou ne peut pas être partagé, téléchargé ou conservé sur les systèmes de l'entreprise. Incluez des exemples de renseignements sensibles, comme les données des clients, les documents comptables, les mots de passe, et les fichiers confidentiels. Assurez-vous que les employés ont bien saisi quelles plateformes et quels outils ont été approuvés pour le partage des fichiers et pour la communication interne. Interdisez l'utilisation des courriels personnels et des applications non autorisées pour les données d'affaires. Passez en revue et mettez à jour régulièrement ces lignes directrices vu que les technologies et les cybermenaces sont en évolution. Et, surtout, veillez à assurer la formation continue des employés afin de renforcer les saines pratiques de manutention de l'information

6. Installation d'un coupe-feu

Installez un coupe-feu pour protéger le système de votre entreprise du trafic malveillant sur Internet.

Le coupe-feu balaie le trafic sur votre réseau et bloque les mouvements indésirables. Le site Pensez cybersécurité du gouvernement fédéral explique le rôle du coupe-feu dans le processus de sécurité.

7. Utilisation d'une passerelle RPV

Prévoyez une passerelle RPV (réseau privé virtuel) pour que vous et vos employés ayez un accès à distance sécurisé et chiffré au réseau de l'entreprise. Le site Web du Centre canadien de cybersécurité explique comment fonctionnent les RPV et liste les divers genres de RPV.

8. Éducation des employés

L'une des principales lignes de défense contre les cyberattaques est une main-d'œuvre sensibilisée à la cybersécurité.

Veillez à l'adoption de politiques et de procédures destinées à la gestion des données propres à votre entreprise et offrez à vos employés des conseils sur la cybersécurité qui soient simples, pratiques et facilement applicables. En cas d'atteinte à la cybersécurité de votre entreprise, vos employés devraient être fin prêts à agir.

Assurez une formation à vos employés afin qu'ils soient au fait de toutes les nouveautés en cybersécurité. Ainsi, tout le monde comprendra son rôle dans sa propre protection et la protection de l'entreprise.

Votre liste de vérification de la cyberhygiène

- [ ] Installation des outils de sécurité adéquats
- [ ] Création de mots et de phrases de passe distincts et compexes
- [ ] Mises à jour des systèmes d'exploitation et des applications
- [ ] Programmation des sauvegardes régulières
- [ ] Désactivation des réseaux de partage de fichiers
- [ ] Installation d'un coupe-feu
- [ ] Utilisation d'une passerelle RPV
- [ ] Sensibilisation des employés

Survol des arnaques les plus fréquentes

Les propriétaires et administrateurs de petites entreprises doivent savoir identifier et garder à l'œil un ensemble d'arnaques destinées principalement aux petites entreprises. Notamment :

- Hameçonnage et fraude par courriel
- Rançongiciel
- Usurpation de l'identité de dirigeants
- Fraude du courriel d'entreprise compromis
- Arnaques du code à usage unique
- Arnaques vocales

Il est utile de connaître les tactiques utilisées par les cybercriminels pour vous leurrer, vous et vos employés, en vue de leur révéler des renseignements importants sur l'entreprise.

INGÉNIERIE SOCIALE : ne vous laissez pas duper

L'ingénierie sociale est le processus par lequel des criminels exploitent la nature humaine – et notre soif de répondre aux demandes urgentes, d'être utiles ou d'aider un ami dans le besoin – afin de leurrer leurs victimes dans la perspective d'obtenir des renseignements personnels qui seront utilisés aux fins de fraude financière.

Lorsqu'il s'agit de cybersécurité, les systèmes de sécurité informatique les plus performants ne peuvent rien contre le fait que des utilisateurs dupés révèlent leurs coordonnées de connexion ou autres renseignements personnels.

Au lieu d'utiliser les techniques de piratage et mener une cyberattaque, les criminels utilisent l'ingénierie sociale pour manipuler psychologiquement, dans l'espoir de faire croire leurs histoires.

3 signaux d'ingénierie sociale

01 Usage de la peur comme motivation. Les courriels, les appels et les textos menaçants ou intimidants sont des techniques d'ingénierie sociale utilisées afin de motiver le receveur à accéder aux demandes de renseignements personnels ou de fonds.

02 Courriels ou textes suspects. Ces messages, qui contiennent des demandes urgentes pour des renseignements personnels, sont une flagrante indication qu'on essaie de vous arnaquer.

03 Offres impossibles à croire ou comportant des demandes inhabituelles. Attention, si un de vos contacts en ligne vous offre un accès gratuit à une application, à un jeu ou à un programme en échange de vos coordonnées de connexion! Également, les offres gratuites en ligne comportent souvent une logique malveillante.

Protection contre les tentatives d'hameçonnage

On ne peut plus se fier aux fautes d'orthographe et de grammaire pour savoir qu'il s'agit d'un courriel hameçon. De nos jours, les fraudeurs connaissent l'importance de soigner leur style, surtout lorsque la cible est une petite entreprise.

Voici quelques signes révélateurs d'un courriel frauduleux.

Exigences et menaces

La demande de renseignements vient-elle d'une source légitime? Votre banque ne vous enverra jamais de courriel menaçant ni ne vous téléphonera pour exiger la divulgation de renseignements personnels, comme votre mot de passe ou le numéro de votre carte de débit ou de crédit. Les fraudeurs se servent d'un langage menaçant pour essayer de vous convaincre de leur révéler des renseignements sensibles.

Expéditeurs douteux

Vérifiez l'adresse électronique de l'expéditeur. Si vous placez votre curseur au-dessus du nom sans cliquer, l'adresse électronique apparaîtra. Certaines tentatives d'hameçonnage utilisent des adresses électroniques qui peuvent sembler légitimes, mais ne le sont pas. La meilleure façon pour en avoir le cœur net est de voir si le nom de domaine du courriel correspond au nom de l'organisation d'où il est censé provenir. Cherchez aussi un léger changement dans une lettre, un symbole ou dans le domaine.

Avertissements

Ne donnez pas suite aux avertissements de fermeture de votre compte, de limitation de l'accès à votre compte ou d'interruption des services si vous ne répondez pas au message. Il s'agit d'une tentative d'hameçonnage.

Testez vos habiletés à reconnaître une fraude avec les questionnaires interactifs de l'ABC
cba.ca/consommateurs/questionnaires-anti-fraude

Pièces jointes et liens douteux

Vous devez toujours vous méfier des pièces jointes et des liens auxquels vous ne vous attendez pas. Les courriels frauduleux souvent prétendent inclure des factures, des notifications et autres, qui semblent valides. Ces liens intégrés semblent anodins, mais peuvent en fait vous mener à des sites frauduleux ou au téléchargement de codes malicieux sur votre appareil.

Des remerciements ou des messages de confirmation de commande non sollicités

Vous pourrez recevoir un message vous remerciant pour un récent achat dont vous ne vous souvenez pas ou une confirmation d'une commande que vous n'avez pas faite. Y répondre pourra exposer votre entreprise à des risques. Si vous avez des doutes, vérifiez vos relevés ou effectuez une recherche sur l'entreprise pour en vérifier la légitimité. S'il s'agit d'une organisation légitime, contactez-la directement au moyen des coordonnées qu'elle affiche sur son site Web. N'utilisez pas les coordonnées incluses dans le message douteux. Restez toujours sur vos gardes.

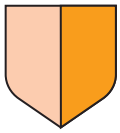
Ce que peuvent faire les propriétaires et gestionnaires de PME

- Sensibiliser à l'hameçonnage dès l'étape de l'intégration et dans les formations.
- Limiter l'accès aux comptes et aux systèmes sensibles aux seuls membres du personnel qui doivent absolument y accéder.
- Créer un processus clair pour le signalement des messages, des courriels et des appels suspects.

Rançongiciels

Un rançongiciel est un logiciel malveillant, ou maliciel, qui bloque l'accès à votre ordinateur ou à vos fichiers, et vous demande une rançon.

Un rançongiciel prend le contrôle de votre appareil et vous en interdit l'accès soit complètement, soit seulement à certains fichiers. Les fraudeurs demanderont une rançon pour vous y redonner accès. Ces menaces visent à vous effrayer et à vous intimider. Le paiement de la rançon ne garantit pas le décryptage de vos fichiers ni n'empêche la vente ou la fuite de vos données en ligne. De plus, vous pourrez vous retrouver, vous et votre organisation, sujets à de nouvelles attaques.



Comment protéger votre entreprise des rançongiciels

Installez des logiciels de protection antivirus et anti-maliciels sur vos appareils et votre réseau, et gardez ces logiciels à jour. Actionnez la mise à jour automatique et ne manquez aucune mise à niveau.

Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications.

Utilisez l'AMF pour tous vos systèmes et comptes afin d'ajouter une couche de sécurité.

Sauvegardez fréquemment vos fichiers sur des systèmes de stockage externes, comme un disque dur ou une plateforme infonuagique, qui ne sont pas reliés à votre ordinateur. S'ils le sont, vos données ainsi sauvegardées pourraient être compromises durant l'attaque.

Faites preuve de prudence! Ne cliquez pas sur des liens ni n'ouvrez des pièces jointes provenant d'adresses inconnues, et désactivez les macros.

Vous pourriez, par inadvertance, télécharger des maliciels en activant des macros, ou en cliquant sur une pièce jointe, un lien ou une fenêtre contextuelle en ligne.

Que faire si vous en êtes victime?

Il serait bien difficile de déverrouiller vos fichiers et de supprimer le rançongiciel de votre système informatique. Si votre entreprise est victime d'un rançongiciel, envisagez les actions suivantes :

Ne payez pas la rançon. Sinon, vous ouvrez la voie à des attaques additionnelles. Les criminels profiteront de votre acceptation de payer la rançon afin de demander plus d'argent.

Déconnectez tous vos appareils. Les rançongiciels peuvent se propager rapidement entre appareils et réseaux. Utilisez un réseau privé différent afin de limiter la propagation de possibles rançongiciels dormants. Nettoyez, réinitialisez et mettez à jour tous vous appareils.

Consultez votre fournisseur de logiciel antivirus. Si vous vous connaissez en récupération de données, vous pourrez essayer de supprimer les logiciels malveillants vous-même. Certains fournisseurs peuvent déceler ce maliciel et offrir des instructions et des logiciels pour remédier au problème.

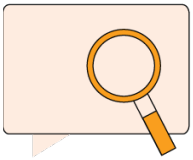
Consultez un spécialiste de la sécurité informatique. Un professionnel peut être en mesure de vous aider à supprimer le rançongiciel et à restaurer vos fichiers si vous les avez sauvegardés.

Changez vos coordonnées compromises. Changez toutes vos coordonnées et vos mots de passe en ligne, en particulier ceux qui donnent accès aux comptes bancaires en ligne de l'entreprise. Ainsi, les criminels ne pourront pas facilement accéder à vos comptes s'ils arrivent à découvrir vos mots de passe.

Signalez la fraude. Informez-en le service de police du quartier, le Centre antifraude du Canada et vos institutions financières.

Fraude du faux dirigeant

La fraude ou arnaque du faux dirigeant, aussi connue sous diverses appellations comme arnaque du PDG ou fraude du président, est une forme de fraude appelée « harponnage ». Il s'agit de la fraude la plus coûteuse pour une organisation. Contrairement à l'hameçonnage, le harponnage est ciblé. Le fraudeur usurpe l'identité d'un haut dirigeant dans une entreprise pour exercer de la pression sur des employés afin qu'ils transfèrent des fonds ou communiquent des informations financières sensibles.



Fonctionnement de l'arnaque

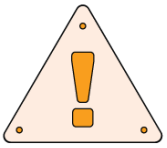
Le fraudeur envoie habituellement un message de la part d'un dirigeant de l'entreprise, notamment le chef de la direction ou le directeur financier, à des employés dans le Service de la comptabilité ou le Service des finances. Le message, qui a l'air complètement légitime, contient une requête urgente et hautement confidentielle. L'usurpateur se sert des tactiques d'ingénierie sociale pour mettre la main sur des données financières hautement confidentielles.

Enregistrements audio ou vidéo générés par l'IA

L'usage des outils de l'intelligence artificielle (IA) peut rendre l'arnaque des dirigeants plus véridique. Grâce à l'IA, les arnaqueurs sont en mesure de créer des enregistrements audio et vidéo qui imitent à perfection la voix et l'apparence de hauts dirigeants de n'importe quelle organisation. Les fraudeurs se servent des enregistrements postés en ligne pour créer des messages audio et vidéo hypertruqués, générés par l'IA, qui semblent refléter l'image et la voix de la personne dont ils usurpent l'identité.

Signes d'arnaques audio et vidéo générées par l'IA

- La vidéo paraît légèrement affectée, avec des mouvements faciaux rigides.
- La voix semble trop limpide et le débit est pointillé de pauses étranges.
- Le message insiste sur le transfert de fonds ou la prise de décision, tout comme dans une arnaque traditionnelle.



Protégez votre entreprise

- **Formez vos équipes** – Sensibilisez les employés à cette arnaque et demandez-leur de se méfier des demandes urgentes ou suspectes envoyées par courriel. Encouragez-les à communiquer avec leur supérieur s'ils pensent qu'une demande est inhabituelle.
- **Confirmez toujours la véracité des demandes** – Si vos employés ou vous-même avez des doutes quant à l'authenticité d'un courriel envoyé par une personne au sein de votre entreprise, entrez directement en contact avec elle par téléphone avant de répondre au courriel, pour vous assurer que la demande est légitime.
- **Instaurez une double approbation des virements** – Adoptez des politiques et des moyens de contrôle pour que plus d'un dirigeant approuve les virements de fonds.
- **Limitez les renseignements partagés en ligne** – En tant que propriétaire d'entreprise, faites attention à ce que vous partagez sur les réseaux sociaux. Les fraudeurs effectuent des recherches poussées sur les particuliers et les organisations, et utilisent des données précises pour vous faire tomber dans leur piège.

Fraude du courriel d'entreprise compromis

La fraude du courriel d'entreprise compromis se présente sous divers types de fraude avancés et vise les entreprises de toutes tailles.

Voici comment identifier les fraudes visant votre entreprise :

Faux dirigeants

Des courriels frauduleux semblent provenir du chef de la direction ou du chef des finances de l'entreprise – ou d'un autre dirigeant –, adressés à un employé du service de la comptabilité ou des finances. Dans ces courriels, le supposé haut dirigeant intime au récipiendaire de virer des fonds à une tierce partie, dans l'immédiat et en toute confidentialité.

Hameçonnage des fournisseurs

Des courriels frauduleux semblent provenir d'un fournisseur avec lequel votre entreprise entretient une longue relation de travail. Dans ces courriels, le prétendu fournisseur vous demande d'effectuer le paiement d'une facture par transfert électronique de fonds à un compte frauduleux.

Vol de renseignements

Des criminels font des demandes, légitimes en apparence, pour des renseignements financiers essentiels, comme des déclarations fiscales, ou autres renseignements confidentiels au sujet de l'entreprise. Ces renseignements serviront à commettre des actes frauduleux.

Comment éviter les fraudes par courriel visant l'entreprise

Éducation

Apprendre aux employés à rester vigilants, car les comptes électroniques de l'entreprise peuvent être compromis, et leur montrer comment détecter ces arnaques. Le signal d'alarme le plus retentissant pour ce genre de fraude est la demande urgente d'un transfert électronique de fonds.

Vérification

Dans le cas de transferts électroniques de fonds, le Centre antifraude du Canada recommande aux entreprises d'établir un processus de vérification à deux étapes afin qu'il y ait un second responsable qui pourra confirmer la validité de la demande.

Prudence

Les renseignements qui seront affichés en ligne ou dans les médias sociaux au sujet des déplacements des hauts dirigeants de l'entreprise pourront être utilisés par des criminels. Il faut toujours être méfiant durant ces périodes.

Protection

Les logiciels de protection – antivirus et autres – doivent, en tout temps, être à jour et fonctionnels sur tous les ordinateurs, appareils informatiques et serveurs de l'entreprise. Vous devez également protéger le domaine de courriel. Utilisez un logiciel contre l'hameçonnage qui correspond au protocole DMARC.

Si votre entreprise est victime...

Aussitôt que vous apprenez qu'un transfert de fonds a été fait à la suite d'une demande frauduleuse, communiquez avec votre banque et signalez l'incident à la police.

Arnaques du code à usage unique : comment doivent réagir les PME

Les arnaques du code à usage unique (OTP) sont progressivement utilisées par les criminels dans les tentatives d'accès aux comptes en ligne. Les PME sont particulièrement visées.

Une entreprise ciblée par ce type d'arnaque peut voir plus d'un seul compte compromis. En effet, les systèmes de paiement, les plateformes bancaires, les comptes de courriel et les données des clients peuvent tous être affectés, ce qui mènera, en fin de compte, à une perturbation des activités, coûteuse pour l'entreprise en termes de temps et d'argent.

Voici quelques mesures pratiques pour vous aider à vous protéger et à protéger votre entreprise.

Fonctionnement de l'arnaque

Dans de nombreuses entreprises, la connexion aux comptes nécessite la saisie d'un code à usage unique (souvent un code numérique), envoyé par SMS, par courriel ou sur une application d'authentification, en vue de vérifier l'identité de l'utilisateur. Le code à usage unique, dont la période de validité est courte, représente une autre couche de sécurité qui s'ajoute aux coordonnées de connexion (nom d'utilisateur et mot de passe). Cette étape dans le processus d'authentification est destinée à renforcer la sécurité des usagers dont le mot de passe a été compromis, en limitant l'accès au compte au seul détenteur du code.

Ainsi, les fraudeurs appellent ou envoient des messages textes en se faisant passer pour des représentants d'organisations légitimes, comme le bureau de poste, la banque, ou une autre organisation de confiance, et demandent le code à usage unique qui vient de vous être envoyé.

Si vous recevez un appel ou un texto douteux, vous demandant de révéler le code à usage unique, envisagez les actions suivantes.

- Ne jamais donner votre code à usage unique à quiconque, encore moins à une personne qui vous appelle, vous texte ou vous écrit pour le demander. Le code à usage unique qui vous est envoyé est exclusivement pour votre usage personnel.
- La réception d'un code que vous n'avez jamais demandé peut s'avérer une tentative par un fraudeur d'accéder à vos comptes. Communiquez avec l'entreprise en question, par des moyens autres que ceux qui sont proposés dans le message douteux, pour signaler la fraude.
- Rappelez-vous que ni votre banque, ni votre fournisseur de services de paie, ni aucune autre organisation respectable ne vous demandera de lui communiquer votre code à usage unique par téléphone, par texte ou par courriel.
- Veillez à ce que les employés qui ont accès aux systèmes d'affaires sachent comment fonctionne l'arnaque par code à usage unique et comprennent que le partage d'un code, ne serait-ce qu'une seule fois, peut mettre l'entreprise en danger.

Si vous croyez que votre entreprise est victime de fraude

Les banques ne ménagent aucun effort afin de protéger les comptes commerciaux qu'elles gèrent et de vous aider à protéger vos comptes. Mais il est essentiel d'agir vite.

Si vous ou l'un de vos employés avez possiblement communiqué un code à usage unique ou des données sensibles à des fraudeurs, envisagez ce qui suit.

- Communiquez avec votre banque et autres institutions financières dans l'immédiat.
- Modifiez les coordonnées de connexion associées aux comptes, qui ont été compromises.
- Assurez-vous d'utiliser un mot (ou une phrase) de passe unique pour chacun de vos comptes en vue d'éviter le bourrage d'identifiants.
- Activez l'authentification multifactorielle sur vos comptes.

Protection contre l'hameçonnage vocal

La fraude téléphonique revêt diverses formes qui reposent sur des tactiques similaires. Un appel convaincant peut mener à des paiements non autorisés, au vol de coordonnées ou à la perturbation des services que vous offrez à vos clients.

Fonctionnement de l'arnaque

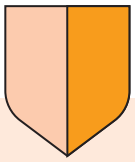
Vous ou l'un de vos employés pourrez recevoir un appel d'un criminel qui se fait passer pour un représentant des forces de l'ordre ou d'une institution financière. Cet individu vous annonce que vous devez de l'argent, que votre entreprise est sous enquête ou que des activités suspectes ont été détectées dans vos comptes financiers corporatifs.

L'appel ou le message vocal ou texte semble authentique. Or, les indications flagrantes qu'il s'agit d'une fraude ne manquent pas.

Les appels et messages utilisent un ton urgent et un langage menaçant afin de vous faire peur et vous forcer à payer la supposée dette ou à révéler vos coordonnées de connexion.

Les appels ou messages comportent des menaces de vous signaler à la police ou de vous trainer en justice si vous ne donnez pas suite à leurs demandes.

Votre correspondant exigera le paiement de votre dette par carte-cadeau, par cryptomonnaie ou par virement de fonds.



Protégez-vous

Les banques s'efforcent de protéger les informations personnelles que vous leur confiez et de vous aider à les protéger vous-même également. Ni les banques ni les organismes gouvernementaux ne vous demanderont le règlement d'une dette ou d'une facture par cartes-cadeaux ou cartes prépayées. Lorsque vous recevez un appel ou un message non sollicité où on vous demande des informations sensibles, envisagez les actions suivantes.

- Ne révélez pas de mots de passe, de numéros de compte ni de codes de vérification.
- Ne réglez jamais un paiement au moyen de cartes-cadeaux, de cartes prépayées, de cryptomonnaies ou de virements électroniques.
- Confirmez la provenance de toutes les demandes de paiement et requêtes relatives aux comptes en communiquant directement avec l'organisation concernée au moyen des coordonnées officielles qui figurent sur son site Web.
- Veillez à ce que les employés qui s'occupent des finances et des comptes clients soient bien formés et sensibilisés aux fraudes téléphoniques et aux mesures de protection des informations sensibles.

Protection des données personnelles des clients

Souvent, les petites entreprises sont visées par les cybercriminels qui croient que ces entreprises n'ont ni les ressources ni les connaissances nécessaires pour adopter les mesures de cybersécurité pertinentes.

À titre de petite entreprise, deux de vos plus importants atouts sont votre personnel et les renseignements financiers de vos clients qui sont en votre possession. Vos clients ont confiance que vous garderez leurs données en sécurité et que vous disposez des procédures et des processus adéquats à la protection de leurs renseignements personnels contre les cybercriminels.

À cette fin, vous devrez suivre une méthode de classification des renseignements de nature délicate et émettre des lignes directrices pour que vos employés sachent comment traiter de tels renseignements.

1. Classifiez et étiquetez correctement vos données sensibles

La première mesure de protection des données de nature délicate que votre entreprise détient est la classification et l'étiquetage adéquats de ces données. Procurez à vos employés les formations nécessaires et renforcez les mesures de classification pertinentes afin de veiller à ce que les données de votre entreprise soient traitées en toute sécurité. La section 7.3 du Guide Pensez cybersécurité pour les petites et moyennes entreprises donne les recommandations suivantes pour un simple modèle de classification :

Renseignements publics

Ces données sont accessibles à tous dans votre entreprise aussi bien qu'à l'extérieur et n'exigent pas de protection, de marquage ou de traitement particuliers; par exemple, articles publiés sur le site Web de votre entreprise.

Renseignements restreints

N'étant pas publics, ces renseignements doivent être étiquetés et protégés. Cette catégorie comprend les fichiers et les données qui ne sont accessibles que par vos employés et vos fournisseurs; par exemple, les dossiers des clients.

Renseignements confidentiels

Ces renseignements étant de nature délicate, seuls peuvent y accéder les employés désignés. Les renseignements confidentiels doivent être étiquetés et protégés, et des restrictions doivent être imposées sur la façon dont ils peuvent être traités; par exemple, les renseignements financiers propres à votre entreprise et à vos clients.

Protection des données personnelles des clients (Suite)

2. Développez un processus de traitement

Ensuite, élaborez un processus pour le traitement des renseignements de nature délicate (restreints et confidentiels) relatifs à votre entreprise et à vos clients. Votre protocole doit comprendre des mesures pour conserver adéquatement les renseignements personnels et préciser quels employés dans votre entreprise peuvent y avoir accès.

3. Vérifiez les politiques et procédures

Assurez-vous d'avoir des politiques et des procédures en place au cas où des renseignements restreints ou de nature délicate se retrouvent compromis. Veillez à ce que vos employés sachent quoi faire dans le cas d'un incident de cybersécurité et organisez régulièrement une formation sur les procédures de cybersécurité.

4. Mettez en place des systèmes de désinfection et de destruction

Enfin, mettez en place un système pour protéger les appareils et détruire les dossiers dont vous n'avez plus besoin. Ainsi, vous empêcherez l'accès non autorisé aux renseignements personnels.

Ressources pour protéger les renseignements personnels de vos clients

Centre canadien de cybersécurité

Sécurité pour les petites et moyennes organisations

Protection de l'information de grande valeur : Conseils pour les petites et moyennes organisations (ITSAP.40.001)

Contrôles de cybersécurité de base pour les petites et moyennes organisations

Pensez cybersécurité

Sections 7.3 et 7.4 du Guide Pensez cybersécurité pour les petites et moyennes entreprises

Commissariat à la protection de la vie privée du Canada

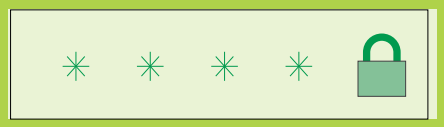
Guide sur la protection de la vie privée à l'intention des entreprises

Cybersécurité : conseils pour vos employés

CANADIAN BANKERS ASSOCIATION

Il est important de prévoir, dans le plan de cybersécurité, une formation de base continue et formelle pour vos employés. En effet, les employés sont très souvent le premier rempart contre les incidents qui menacent la cybersécurité.

Commencez par des conseils simples, pratiques et faciles à appliquer. La prévention des cybermenaces est un sport d'équipe auquel tout le monde participe. Prenez note de ces simples renseignements...



Votre première ligne de défense

Utilisez une phrase ou un mot de passe exclusif pour accéder au réseau de l'entreprise et modifiez-le régulièrement.

Signes que le courriel que vous venez de recevoir est un hameçon

Demandes inhabituelles de la part d'un fournisseur

Des cybercriminels peuvent envoyer des courriels similaires à ceux de l'un de vos fournisseurs fiables. Généralement, de tels courriels vous demanderaient de transférer le paiement d'une facture électroniquement à un compte frauduleux. Vérifiez toujours l'adresse de l'expéditeur : il suffit de placer le curseur par-dessus sans cliquer; la vraie adresse électronique apparaîtra. Si le domaine de l'adresse ne correspond pas à l'organisation, vous saurez immédiatement qu'il s'agit d'une fraude.

Exigences et menaces

La demande de renseignements est-elle valable? La banque n'enverra jamais un courriel menaçant ni n'appellera pour demander des renseignements personnels, comme le mot de passe, le NIP de vérification du compte, le nom de jeune fille de votre mère ou les numéros des cartes de paiement.

Demandes irrégulières de renseignements

Aussi, les cybercriminels peuvent essayer d'obtenir des renseignements financiers confidentiels, comme les déclarations de revenus, qu'ils utiliseront afin de commettre des fraudes.

Avertissements

Des avertissements au sujet de la fermeture de votre compte ou de la restriction de votre accès au cas où vous ne répondez pas aux demandes faites dans le courriel sont un autre signal d'hameçonnage.

Pièces jointes ou liens douteux

Ne jamais cliquer sur une pièce jointe ou un lien douteux. Il faut toujours se méfier des messages non sollicités comprenant du contenu intégré. Les courriels frauduleux contiennent souvent des liens intégrés frauduleux qui semblent provenir de sources légitimes. Passer le curseur par-dessus le lien aide à en identifier la source. Or, si vous passez le curseur par-dessus une adresse frauduleuse, ce qui apparaîtra ne sera pas reconnaissable. Vous saurez qu'il s'agit d'un courriel hameçon lorsque l'adresse ne correspond pas ou contient des irrégularités.

Demandes bizarres de la part du propriétaire de l'entreprise ou d'un membre de la haute direction

Les cybercriminels peuvent usurper les adresses électroniques des employés. Un signal flagrant d'une possibilité de fraude par courriel d'entreprise compromis est la demande d'un transfert électronique qui semble provenir de l'adresse du propriétaire ou d'un haut gestionnaire et qui incite à agir sans tarder.

Encore des recommandations...

- Soyez méfiants des appels et des visites de la part d'individus demandant des renseignements au sujet de l'entreprise ou des employés. Les criminels recherchent souvent des renseignements personnels sur les employés en vue de lancer une cyberattaque.
- Dans le doute, consultez votre superviseur ou demandez l'aide d'un collègue.
- Signalez tout événement suspect à votre superviseur. Très souvent, c'est ainsi qu'on fait échouer une cyberattaque.
- Si vous croyez que l'information bancaire a fuité, signalez-le immédiatement afin que l'institution financière puisse être avisée et que les comptes de l'entreprise soient protégés contre tout accès frauduleux.

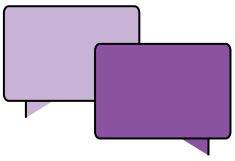
Signaler la fraude

Si jamais vous croyez avoir été victime d'une tentative de fraude, vous devrez la signaler tout de suite. Ainsi, vous contribuerez à la protection de tout le monde, autant vous que les autres : les escrocs auront plus de difficultés à exécuter leurs activités frauduleuses.

Pourquoi signaler la fraude?

1. **Protéger autrui.** Lorsque vous signalez une activité frauduleuse, vous contribuez à attirer l'attention d'un plus grand nombre de personnes et donc à les protéger.
2. **Éliminer les escrocs.** Les forces de l'ordre et les agences de prévention de la fraude utilisent les signalements pour suivre et arrêter les escrocs. Plus elles disposent de données grâce aux signalements, plus elles sont efficaces.
3. **Protéger son argent.** Signaler la fraude aussitôt que possible aide à sécuriser les comptes et à réduire les risques de vol.

Quelques types d'activités frauduleuses fréquemment signalées



Hameçonnage par message texte

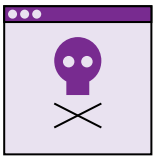
Vous recevez un message texte qui, souvent, semble parvenir d'une organisation connue, comme votre banque ou bien un organe fédéral ou provincial.

Hameçonnage par courriel

Dans ce type de fraude, les criminels essaient de vous faire croire que le message provient d'une personne ou organisation fiable afin que vous cliquiez sur le lien frauduleux qu'il contient, ce qui leur facilitera la tâche de voler vos renseignements personnels ou financiers.

Appels frauduleux

Un escroc se fait passer pour un employé de votre banque, un fonctionnaire ou même l'un de vos proches dans le pétrin, avant de vous servir une raison fallacieuse pour vous demander d'envoyer de l'argent ou de révéler vos renseignements personnels.



Sites Web frauduleux

Ces sites ont l'air authentiques, mais ils sont plutôt des pièges destinés à voler vos données personnelles, les renseignements sur votre carte de crédit et votre argent.

Signaler la fraude (Suite)

Signaler une activité frauduleuse

1. Signalement au Centre antifraude du Canada (CAFC)
Le CAFC recueille les signalements de tous les types de fraude. Un signalement au CAFC contribue à protéger tout le monde, autant vous que les autres.

En ligne : Système de signalement de la fraude
Par téléphone : 1-888-495-8501

2. Signalement à votre banque
Si vous avez communiqué des renseignements personnels ou transmis de l'argent à la suite d'une fraude, contactez immédiatement votre banque ou le fournisseur de votre carte de crédit. Ces organisations peuvent contribuer à arrêter une transaction et à mettre votre compte à l'abri.

3. Signalement des pourriels
Vous pouvez signaler les pourriels facilement et gratuitement en les transférant par texto au 7726 (SPAM). Ainsi, vous contribuerez à l'identification de nouveaux types de pourriels et à l'amélioration des filtres utilisés par votre fournisseur de téléphonie mobile pour bloquer les pourriels nocifs. PensezCybersécurité présente des renseignements additionnels au sujet du signalement des pourriels par messages textes au 7726, ainsi que du signalement sur appareils Android et iOS.

4. Signalement des sites Web frauduleux au Bureau de la concurrence
Si vous tombez sur un site Web frauduleux, veuillez le signaler au Bureau de la concurrence, organisme chargé de contribuer à l'application de la loi en cas de pratiques malsaines sur le marché.

En ligne : Signalements des fraudes au Bureau de la concurrence

5. Signalement au service de police
Si la tentative de fraude s'est soldée par une grande perte financière ou par un vol d'identité, vous devrez signaler l'événement également au service de police de votre localité. La plupart des services de police acceptent les signalements de fraude non urgents, en ligne ou par téléphone.

À faire après le signalement

- **Conservez les documents** – Préservez toutes les communications en lien avec la fraude et documentez tous les signalements que vous faites.
- **Surveillez vos comptes** – Guettez toute activité anormale sur vos comptes bancaires, vos cartes de crédit et vos comptes en ligne.
- **Restez à jour** – Consultez le site Web du Centre antifraude du Canada pour les mises à jour régulières sur les activités frauduleuses en cours. Également, abonnez-vous au bulletin électronique gratuit *Conseils sur la prévention de la fraude* de l'Association des banquiers canadiens.

Le signalement des stratagèmes frauduleux est l'un des meilleurs moyens dont vous disposez pour vous protéger et protéger vos proches. Les quelques minutes que vous y investissez rapportent gros. En cas de doute quant à la présence d'une fraude, il est préférable de faire un signalement et de laisser les spécialistes en décider. Lorsque nous tous restons sur nos gardes et signalons les activités suspectes, les escrocs auront plus de difficultés à exécuter leurs activités frauduleuses.

Ressources additionnelles

Association des banquiers canadiens
Prévention de la fraude :
cba.ca/fraude

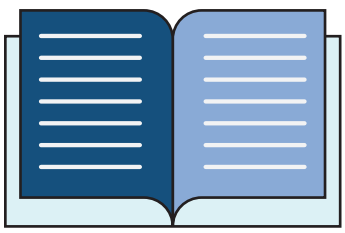
Association des banquiers canadiens
Bulletin gratuit sur la prévention de la fraude :
Abonnement en ligne.

Coalition canadienne antifraude
EnsembleContrelaFraude.ca

Gouvernement du Canada
Pensez cybersécurité :
Pensez cybersécurité pour les petites et moyennes entreprises

Centre canadien pour la cybersécurité
Cybersécurité pour les petites et moyennes organisations

Votre banque pourrait avoir des ressources additionnelles. Voyez avec votre institution financière quels sont les services, les guides et les conseils en matière de sécurité offerts aux petites entreprises clientes.



ASSOCIATION DES BANQUIERS CANADIENS

L'Association des banquiers canadiens est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiennes et Canadiens à atteindre leurs objectifs financiers. cba.ca

PENSEZCYBERSECURITE.CA

Pensez cybersécurité est une campagne nationale visant à informer les Canadiens sur les enjeux de la cybersécurité et à leur indiquer des façons simples de se protéger en ligne. Cette campagne est menée au nom du gouvernement du Canada par le Centre de la sécurité des télécommunications qui profite de l'expertise de son Centre canadien pour la cybersécurité. Pensezcybersecurite.ca