L’art de la prévention des fraudes

Comment protéger votre entreprise et votre clientèle

Par Diane Amato, pour RBC

C’est de votre entreprise qu’il s’agit.

Vous n’avez ménagé aucun effort pour la bâtir et vous êtes prêt à tout pour assurer son avenir. Personne n’a le droit de voler votre argent, vos données ou vos clients. Vous avez travaillé très fort pour bâtir votre entreprise, et vous devez maintenant travailler tout aussi fort pour la protéger.

Soyons francs, la fraude – et les risques qu’elle peut comporter pour votre entreprise et vos résultats financiers — n’est pas un enjeu à prendre à la légère. On est facilement tenté de mettre le sujet en veilleuse, en se disant qu’on pourra toujours y revenir plus tard. Sans vouloir être alarmiste en parlant de pirates informatiques, de fraudeurs ou de comptables mal intentionnés qui pourraient faire obstacle à la réussite de votre entreprise, il faut tout de même mentionner que le fait d’ignorer les risques réels de fraude en entreprise peut avoir de graves conséquences.

À l’intérieur

Pourquoi garder un œil sur la prévention de la fraude 3

Le cybercrime et votre entreprise
Les menaces criminelles et les mesures à prendre à leur sujet 4

La fraude sur paiement
Une arnaque traditionnelle constamment mise à jour 6

Piratage psychologique
La politesse pourrait vous coûter cher 8

La fraude sur chèque
Encore monnaie courante 10

Fraude interne
Comment protéger votre entreprise contre
une fraude orchestrée de l’intérieur 12

Dix conseils pour protéger votre entreprise contre la fraude 14

Pourquoi garder un œil sur la prévention de la fraude

1 Prévenir la fraude est possible.

Dans bien des cas, c'est même facile. Si vous exploitez une grande entreprise, vous pouvez avoir besoin de systèmes sophistiqués pour assurer la protection complète de vos renseignements. S'il s'agit d'une petite ou moyenne entreprise, cependant, la protection de vos finances et de vos données se résume la plupart du temps à de simples contrôles et à l'établissement de politiques qui contribuent à limiter les risques auxquels vous êtes exposé. Pour des conseils faciles à mettre en pratique, consultez nos Dix conseils pour protéger votre entreprise contre la fraude.

2 La détection de la fraude et la prévention des attaques peuvent contribuer à protéger les capitaux et la réputation de votre entreprise.

Selon la taille de votre entreprise, une protection inadéquate de vos finances, des données sur vos clients et de vos renseignements peut vous faire perdre des milliers – voire des millions — de dollars en capitaux ou en futurs revenus. Qu'il s'agisse de cybercrime, de paiements frauduleux, de fraude par chèque ou d'une escroquerie à l'interne, vous risquez littéralement de tout perdre si votre entreprise est victime de fraude. Est-ce une raison suffisante? Nous pensons que oui.

3 Les fraudeurs sont de plus en plus rusés et sophistiqués.

Vous travaillez fort pour assurer la réussite de votre entreprise. Pendant ce temps, des fraudeurs travaillent fort pour soutirer à votre entreprise des renseignements et de l'argent. Ils passent beaucoup de temps à perfectionner leurs méthodes et conçoivent continuellement de nouvelles façons de duper les gens afin de leur soutirer leur argent. Pour voir à quel point les fraudeurs peuvent faire preuve d'imagination, consultez notre article Piratage psychologique : la politesse pourrait vous coûter cher. Il importe d'être vigilant et de demeurer au fait des techniques utilisées par les fraudeurs pour éviter de figurer au nombre de leurs victimes.

4 Il ne s'agit pas nécessairement d'une préoccupation constante.

Si vous êtes conscient des risques de fraude et que vous vous méfiez de toute activité anormale, vous pourrez mieux prémunir votre entreprise contre une attaque frauduleuse. Pour en savoir plus sur les risques encourus par votre entreprise si vous relâchez votre vigilance, consultez la section Le cybercrime et votre entreprise : les menaces criminelles et les mesures à prendre à leur sujet.

Puisque la prévention de la fraude n'est probablement pas au premier plan de vos préoccupations, suivez l'actualité et consultez les articles et les rapports les plus récents sur le sujet. Les alertes de RBC, par exemple, fournissent les plus récents renseignements concernant la protection des données, la fraude, ainsi que d'autres enjeux liés à la sécurité.

Le cybercrime et votre entreprise

Les menaces criminelles et les mesures à prendre à leur sujet

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

Bien que ce type de crime revête de nombreuses formes, trois d'entre elles devraient retenir l'attention de tout propriétaire d'entreprise.

Partout dans le monde, le cybercrime est maintenant la plus rentable des activités criminelles, et il coûte chaque année plus de 400 milliards de dollars aux entreprises[1].

L'hameçonnage

L'hameçonnage est une forme très répandue d'escroquerie en ligne. Au moyen d'un courriel, on tente d'amener des gens à fournir des renseignements personnels, financiers ou d'entreprise. En général, le courriel d'hameçonnage présente au destinataire une situation urgente (« Notre service d'audit a décelé un problème concernant votre compte »), fixe un délai (« Vous devez vérifier votre compte dans les 24 heures ») et contient un lien vers une page où le destinataire doit fournir des renseignements confidentiels (« afin de régler le problème »). L'hameçonneur peut ainsi obtenir des mots de passe, des numéros de compte ou des noms de clients, ou même accéder aux systèmes informatiques de sa victime. Rappelez-vous qu'aucune organisation légitime ne vous demandera jamais de lui fournir des renseignements de cette manière.

CONSEIL

Les employés sont formés pour offrir un bon service aux clients, ce qui en fait également des cibles pour les hameçonneurs. Assurez-vous qu'ils font preuve de prudence à l'égard des liens dans les courriels et des pièces jointes à télécharger.

Les logiciels malveillants

Les logiciels malveillants (ou maliciels) sont conçus pour infiltrer des systèmes informatiques et causer des dommages, que ce soit en corrompant des fichiers ou des applications, en épiant des activités ou en copiant des données. Les cybercriminels se servent souvent de tels « outils » pour pénétrer dans des systèmes afin de voler de l'argent ou des renseignements. Une intrusion par logiciel malveillant est parfois perceptible à certains signes : lenteur du traitement, disparition de logiciels de protection, ou multiplication des pannes et des cas de gel d'écran. Diverses mesures vous aideront à protéger votre entreprise contre les logiciels malveillants, notamment l'installation d'un antivirus à jour et la suppression des applications désuètes. Et si vous recevez un courriel ou un message texte non sollicité, vous ne devez jamais y donner suite en fournissant des renseignements confidentiels ou en entrant un nom d'utilisateur ou un mot de passe.

Le rançongiciel

Le rançongiciel est l'un des nombreux types de logiciel malveillant. Nous en soulignons l'importance en raison de la fréquence croissante des attaques et du tort énorme qu'elles causent aux entreprises. L'ampleur des dommages tient au fait qu'une fois les systèmes infiltrés, le rançongiciel copie habituellement l'ensemble des fichiers, puis verrouille les systèmes. Les pirates exigent ensuite une rançon pour les déverrouiller. Ce genre d'attaque peut paralyser une entreprise, et il peut falloir des semaines, ou même plus longtemps, pour revenir à la normale. Dans l'intervalle, l'entreprise est parfois incapable d'exercer ses activités. Les mesures de prévention contre les logiciels malveillants sont également efficaces contre les rançongiciels. Toutefois, il ne suffit pas d'être vigilant dans l'utilisation des logiciels et du courriel ; il faut aussi faire régulièrement des copies de sécurité des données de l'entreprise pour qu'elle puisse reprendre rapidement ses activités en cas d'attaque par rançongiciel.

Au-delà de ces dangers bien réels, les entreprises font également face à une grave menace d'un type très différent : l'illusion d'invulnérabilité de certains propriétaires d'entreprise.

Protection de votre entreprise

En réalité, toutes les entreprises courent un risque. Voici quelques conseils qui vous aideront à protéger la vôtre contre les cybercriminels :

1 Faites appel à un expert.

Si la place de la technologie dans vos activités est peu importante et que vos systèmes ne sont pas complexes, vous pourriez vous croire à l'abri des cyberfraudeurs. Toutefois, le simple fait que vos employés communiquent par courriel entraîne un risque. Vous êtes également une cible potentielle si vous faites des achats en ligne. Si vous n'êtes pas doué en informatique, faites appel à une personne fiable qui s'y connaît. Elle s'assurera que vos systèmes sont à jour et dotés d'un antivirus efficace.

2 Informez vos employés.

Vos employés sont probablement des gens charmants à qui vous feriez confiance pour garder vos enfants. Toutefois, même s'ils n'ont pas de mauvaises intentions, ils sont humains, et donc sujets à l'erreur. Un employé peut faire l'erreur de se connecter à l'entreprise à partir d'un café (et ainsi rendre vos données vulnérables sur un réseau non sécurisé), ou encore cliquer dans une fenêtre contextuelle malveillante. À une époque où 90 % des intrusions informatiques résultent d'une erreur humaine, même les employés les plus loyaux peuvent constituer un maillon faible pour une entreprise.

3 N'oubliez pas que vous êtes une cible potentielle.

Si vous pensez que seuls les géants du détail ou de la technologie font l'objet d'intrusions, détrompez-vous. Les pirates peuvent souvent mettre la main sur de l'argent ou des renseignements en s'en prenant à de petites entreprises. Par exemple, ils peuvent rediriger un télévirement destiné à un fournisseur ou se servir de données de votre entreprise pour lancer une attaque contre l'un de vos clients ou de vos fournisseurs. Peu importe la taille de votre entreprise, toute faiblesse peut en faire la cible de fraudeurs.

4 Faites preuve de vigilance.

Ce sont des gens très astucieux et extrêmement sophistiqués qui ne négligent aucune occasion de s'attaquer à une entreprise vulnérable. En infiltrant vos systèmes, ils peuvent surveiller vos échanges de courriels et ainsi connaître vos habitudes, vos contacts, votre façon d'écrire, de même que l'horaire de vos déplacements. Rien de plus simple ensuite que de se faire passer pour une personne en qui vous avez confiance afin de vous convaincre de rediriger un virement vers un autre compte de banque.

5 Augmentez la sécurité de vos mots de passe.

Un mot de passe constitué d'un seul mot auquel on ajoute un ou deux chiffres n'offre pas assez de protection. Choisissez des mots de passe composés de lettres, de chiffres et de caractères spéciaux, et n'utilisez pas le même pour accéder à divers systèmes. Rappelez-vous aussi de changer vos mots de passe régulièrement.

De nos jours, les cybercriminels sont patients et sophistiqués et voient leurs activités non pas comme des crimes, mais comme une carrière. Et comme ils ont accès à des fonds, ils n'ont aucune raison de cesser leurs attaques. La meilleure façon de protéger vos systèmes informatiques est de demeurer vigilant et de mettre en place des mesures de protection. Il vous sera plus facile d'amorcer ce processus après avoir lu nos Dix conseils pour protéger votre entreprise contre la fraude.

La fraude sur paiement

Une arnaque traditionnelle constamment mise à jour

Les premiers télévirements frauduleux remontent à plus de cent ans. Des fraudeurs s'employaient alors à intercepter des virements télégraphiques. La fraude sur paiement a connu une évolution fulgurante depuis ce temps, et englobe aujourd'hui les télévirements frauduleux, la fraude par courriel et la fraude sur chèque. Voici un aperçu des procédés qu'utilisent de nos jours les auteurs de télévirements frauduleux et de fraudes par courriel, ainsi que des façons de protéger votre entreprise contre ces menaces. Nous vous invitons également à lire l'article que nous avons consacré à la prévention de la fraude sur chèque, intitulé La fraude sur chèque : encore monnaie courante.

Bien que les fraudeurs aient recours à diverses astuces pour intercepter ou rediriger des paiements, le mensonge est généralement leur arme de prédilection pour commettre une fraude sur paiement. En mentant au sujet d'une situation, ils amènent des propriétaires d'entreprise ou leurs employés à leur envoyer des paiements ou des virements d'un type ou d'un autre.

CONSEIL

La formation et l'information sont vos outils les plus efficaces pour protéger votre entreprise des fraudes. Les propriétaires d'entreprise doivent veiller à ce que leurs employés adoptent de bonnes habitudes en matière de sécurité, et le faire eux-mêmes.

À l'heure actuelle, la principale menace émergente en matière de fraude sur paiement est un stratagème qu'on appelle l'escroquerie par intrusion dans un courriel d'entreprise. Voici ce que vous devez savoir à ce sujet :

Comment cela fonctionne-t-il ?

Imaginons que vous êtes propriétaire, chef de la direction ou chef des finances d'une entreprise (ou, essentiellement, que vos fonctions vous autorisent à envoyer des sommes importantes). Un fraudeur pourrait mettre la main sur votre information d'authentification de courriel (ou sur d'autres renseignements d'accès en ligne) et ensuite se faire passer pour vous. Il pourrait alors envoyer à l'un de vos employés des instructions lui demandant de diriger un paiement vers un compte bancaire de son choix.

Pourquoi cela fonctionne-t-il ?

Les criminels sont minutieux et font des recherches. Un fraudeur pourra inclure dans un courriel des détails concernant des membres de votre équipe et des projets en cours – et même des projets secrets –, ce qui donnera à son message une apparence de légitimité.

Y a-t-il des variantes courantes de ce type de fraude ?

L'escroquerie par intrusion dans un courriel d'entreprise peut prendre diverses formes. Voici quelques exemples :

L'escroquerie au chef de la direction

Un fraudeur réussit à accéder au compte de courrier électronique du chef de la direction (ou d'un autre cadre supérieur), ou reproduit un domaine Internet afin de donner l'impression qu'un courriel provient des plus hauts échelons d'une entreprise. Il profite des vacances d'un dirigeant pour envoyer en son nom un courriel demandant l'exécution d'une opération financière. En général, il demande qu'on modifie les renseignements ayant trait à l'acheminement des fonds vers un compte, ou encore qu'on effectue un dépôt ou un virement de nature inhabituelle.

Comme il a fait des recherches et a surveillé les courriels, le fraudeur sait à quel moment le chef de la direction sera à l'extérieur de la ville. Il attend donc qu'il soit absent afin que le destinataire ne puisse pas lui parler en personne pour faire confirmer la demande. Le fraudeur ajoute un prétexte plausible justifiant la procédure inhabituelle et la nécessité de garder le secret : « Je prévois faire une annonce dans la matinée. D'ici là, veuillez ne mentionner cette demande à personne. »

La demande de paiement provenant d'un fournisseur

Se faisant passer pour un fournisseur, un fraudeur envoie un courriel à un employé des comptes fournisseurs. L'information relative à son compte a changé, explique-t-il : « Pourriez-vous s'il vous plaît verser le paiement dans notre nouveau compte, dont le numéro est xxxx ? » Ainsi, même si les systèmes de votre entreprise ne sont pas infiltrés, le piratage du compte de courrier électronique de l'un de vos fournisseurs permet au fraudeur de vous envoyer une demande de réacheminement de paiement qui aura l'air légitime.

Le faux avocat

Selon un stratagème similaire, un faux avocat demande à un employé de virer vers un compte frauduleux la somme nécessaire à une opération importante – comme le règlement d'un litige ou le paiement d'une facture en souffrance. Persuadé par le fraudeur que le virement demandé est urgent et confidentiel, l'employé est peu enclin à demander une confirmation à quelqu'un d'autre.

Quels sont les types d'entreprises qui courent un risque ?

L'escroquerie par intrusion dans un courriel d'entreprise est utilisée contre des entreprises de toute taille, et des cas ont été signalés dans 80 pays.

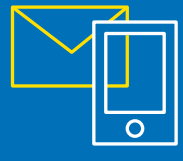
Les entreprises les plus vulnérables sont celles qui font affaire avec des fournisseurs étrangers ou qui effectuent régulièrement des télévirements. Cela dit, les fraudeurs s'adaptent et ils modifient leurs tactiques de façon à pouvoir les utiliser avec d'autres modes de paiement. Toute entreprise doit donc faire preuve de prudence à l'égard des demandes de fonds reçues par courriel.

Comment protéger mon entreprise ?

À l'origine d'une escroquerie par intrusion dans un courriel d'entreprise (ou de toute autre variante de la fraude sur paiement), il y a souvent une erreur humaine en plus du piratage de comptes et de systèmes en ligne. Même si certaines stratégies peuvent facilement être mises en place pour accroître votre niveau de sécurité en ligne, la façon la plus efficace de protéger votre entreprise est sans doute de bien gérer l'élément humain. En définitive, il faut quelqu'un pour envoyer un paiement ou un virement.

CONSEIL

Utilisez un autre moyen de communication pour les vérifications : par exemple, si vous recevez une demande de virement par courriel, vérifiez l'identité de l'expéditeur en lui téléphonant à un numéro que vous savez valide.



Piratage psychologique

La politesse pourrait vous coûter cher

Votre entreprise a beau avoir tous les pare-feu, les antivirus et les experts en cybersécurité souhaitables, elle n'en est pas pour autant immunisée contre la fraude. Il faut aussi prendre en compte le facteur humain, qui peut avoir des effets tout aussi désastreux que les stratagèmes techniques les plus sophistiqués.

Le piratage psychologique mise sur la manipulation des sentiments pour inciter les employés ou les propriétaires d'entreprise à révéler des renseignements importants.

Les pirates sont bien informés

De nos jours, les pirates sont bien informés : ils se renseignent sur les rôles des employés, les partenaires et les processus de l'entreprise visée, puis ils ciblent des employés précis en leur présentant des renseignements, des offres et des questions qui les interpelleront. Des fraudeurs ont peut-être même déjà amorcé la conversation et créé des liens avec une personne de votre entreprise par l'intermédiaire d'un site de réseautage social. Vos employés – surtout ceux qui sont polis, amicaux, conciliants et confiants – pourraient être amenés par la ruse à divulguer des renseignements qui pourraient entraîner des pertes financières ou des fuites d'information.

Voici quelques moyens courants par lesquels les fraudeurs peuvent tenter d'accéder à vos employés :

Prétexte

Le fraudeur trouve un prétexte pour entrer en contact avec un employé et lui demander des renseignements confidentiels ou sécurisés. Par exemple, il peut prétendre être un fournisseur potentiel ou appeler pour le compte d'une entreprise de recherche, d'une banque ou d'un organisme gouvernemental, et demander le nom d'autres employés, des renseignements bancaires, des justificatifs d'ouverture de session ou des renseignements qui peuvent sembler inoffensifs (comme le nom d'un enfant, une date d'anniversaire ou votre fournisseur de téléphonie cellulaire). Les renseignements recueillis peuvent servir à composer un profil permettant au fraudeur de se faire passer pour un employé et d'accéder à vos comptes, à vos systèmes ou à vos clients.

CONSEIL

À moins d'avoir vérifié qu'une personne est autorisée à obtenir des renseignements sur un employé, votre entreprise ou les réseaux de votre entreprise, il est risqué de les lui fournir.

Mystification par téléphone ou par courriel

Il est plus facile que l'on pense de créer une adresse courriel ou un identifiant téléphonique trompeur. De nombreuses personnes se font berner par des appels ou des courriels qui semblent provenir d'une source fiable. La légitimité apparente du nom indiqué sur l'afficheur ou l'adresse courriel ne garantit aucunement que la personne qui communique avec vous est honnête.

Appâtage

Cette technique vise à exploiter la curiosité humaine. Elle utilise la promesse d'une récompense, comme un téléchargement de musique gratuit, si l'employé entre les renseignements que recherche le fraudeur. L'appât peut aussi se présenter sous forme physique.

Méfiez-vous des clés USB trouvées au bureau ou dans un stationnement : des employés curieux pourraient les brancher et infecter vos systèmes par mégarde.

Talonnage

Qui n'a pas déjà laissé entrer quelqu'un qui est derrière soi dans un immeuble ou un bureau ? En se donnant l'apparence d'un livreur ou d'un technicien, un fraudeur peut accéder à des lieux non autorisés s'il trouve une personne bien intentionnée pour lui tenir la porte à l'entrée. Le « talonneur » peut ensuite voler des biens ou des données. Par exemple, il pourrait voler un portable, entrer dans votre salle de serveurs, ramasser des factures contenant des renseignements sur des clients ou des fournisseurs, ou encore brancher un dispositif malveillant sur un poste de travail laissé sans surveillance.

Même si vous avez d'excellents antivirus, la cybersécurité ne suffit pas : vos mesures de prévention de la fraude doivent aussi tenir compte du facteur humain. Étant donné le caractère perfectionné des tactiques de fraude appuyées sur des recherches, vous et vos employés pourriez facilement être victimes de piratage psychologique et compromettre des numéros de compte, des mots de passe, des données sur les clients ou d'autres renseignements.

La protection contre le piratage psychologique repose sur la formation et la sensibilisation des employés. On conseille aussi d'investir dans des services de dépistage en ligne qui peuvent repérer les fausses adresses courriel, les sites Web malveillants et les virus potentiels.

Pour obtenir d'autres conseils sur la façon de mettre en place les bonnes mesures de contrôle au sein de votre entreprise : Dix conseils pour protéger votre entreprise contre la fraude.

La fraude sur chèque

Encore monnaie courante

Le chèque est l'un des modes de paiement les plus anciens, remontant à l'époque romaine au dire de certains. Malgré les avancées dans la technologie des paiements et les différentes options électroniques maintenant offertes, de nombreuses entreprises continuent d'utiliser les chèques. L'utilisation de chèques est en baisse d'environ 5 % par année depuis dix ans, mais les banques canadiennes en traitent encore plus d'un milliard chaque année.

Il n'est donc pas étonnant que la fraude sur chèque soit toujours monnaie courante.

En fait, la fraude sur chèque a fait perdre aux entreprises plus d'argent que tout autre type de fraude au cours des dernières années[2].

(Ce type de fraude est moins courant que d'autres, mais les pertes par incident peuvent être plus importantes).

Comme les chèques devraient être utilisés d'ici au moins 20503, ce type de fraude ne doit pas être négligé.

Comment se fait-il que la fraude sur chèque existe encore ?

La fraude sur chèque existe depuis presque aussi longtemps que les chèques : le problème n'aurait-il pas dû être réglé depuis tout ce temps ? Voici quelques explications :

1 La technologie.

Il est vrai que le secteur des paiements a évolué. L'encre, le papier et les filigranes complexifient la falsification des chèques, mais la technologie est une arme à double tranchant : il est relativement facile (et peu coûteux) de créer, de reproduire ou de falsifier un chèque grâce à la technologie qui permet de créer des chèques contrefaits des plus réalistes, ainsi que les fausses pièces d'identité qui servent à les encaisser.

2 Le faible coût d'entrée.

De quoi un fraudeur a-t-il réellement besoin pour créer un faux chèque ? Rien de très complexe : du papier de haute qualité, une imprimante, un numériseur et une habileté avec Photoshop. Autrement dit, les frais peu élevés associés à cette pratique en font une activité facilement accessible.

3 La facilité d'interception.

Comme les chèques sont des effets physiques, un employé, un facteur, ou un voleur qui fouille dans les boîtes aux lettres, les conteneurs à ordures et les bacs de recyclage peut facilement les intercepter.

Comment les entreprises peuvent-elles se protéger contre la fraude sur chèque ?

Heureusement, il existe des mesures qui peuvent contribuer à protéger votre entreprise. Il s'agit simplement d'appliquer des politiques et des processus qui feront une véritable différence pour la sécurité de vos opérations financières. Voici les pratiques les plus efficaces :

Utilisez des modes de paiement électroniques.

Que ce soit en faisant des télévirements ou des virements, ne plus recourir à un mode de paiement physique peut permettre de réduire le risque de fraude.

Vérifiez chaque jour le solde de vos comptes.

Vous pourrez ainsi repérer rapidement les opérations frauduleuses et avertir votre banque. Et gardez à l'esprit qu'il existe des limites de temps imposées par le gouvernement fédéral pour que la banque du déposant retourne à votre banque le chèque encaissé et débité de votre compte.

CONSEIL

Comme les politiques varient d'une banque à l'autre, plus vite vous découvrez une opération suspecte, meilleures seront vos chances de récupérer les fonds volés.

Utilisez des services automatisés de détection de la fraude.

Des services comme Appariement des bénéficiaires et Vérification des décaissements de même que le service de vérification inverse des décaissements peuvent vous aider à déceler plus rapidement les irrégularités et à faire le rapprochement de vos opérations par chèque.

Verrouillez l'endroit où vous stockez vos chèques.

Ne laissez pas vos chèques à la vue de tous ou dans un endroit non sécurisé. Conservez toujours vos chèques, bordereaux de dépôt, relevés bancaires et autres effets de nature confidentielle en lieu sûr.

Déchiquetez les chèques annulés et les anciens relevés.

Ne donnez pas aux fraudeurs l'occasion de copier les numéros de vos comptes et les renseignements de vos chèques.

Exigez deux signatures.

Exigez que deux personnes autorisées signent tous les chèques ou ceux supérieurs à un montant donné. Cette mesure peut réduire le risque qu'une personne libelle un chèque à son propre nom ou au nom d'une entreprise fictive.

Utilisez différents comptes pour différents services.

En séparant vos comptes, et du coup les chèques que vous tirez, vous simplifiez le suivi de vos paiements et pouvez repérer plus facilement les irrégularités.

Oui, la fraude sur chèque est encore monnaie courante, mais vous pouvez la prévenir. En suivant ces conseils et en renseignant vos employés, vous réduirez les risques pour votre entreprise.

Fraude interne

Comment protéger votre entreprise contre une fraude orchestrée de l'intérieur

La fraude interne peut prendre de multiples formes allant du vol d'argent dans la caisse au détournement de millions de dollars, en passant par la manipulation de chèques et l'écrémage des fournitures de bureau. L'impact sur l'entreprise peut être autant psychologique que financier lorsque l'auteur est une personne en qui l'on avait confiance.

Toutefois, à condition de mettre en place des mesures de contrôle appropriées, on peut généralement débusquer la fraude interne.

Souvent, il suffit d'établir des politiques robustes, d'encadrer l'intégration et le départ d'employés par des mesures de diligence, ainsi que d'éviter de donner trop de pouvoir à une seule personne.

Voici des mesures qui vous aideront à mettre votre entreprise à l'abri de la fraude interne

Mettez en place des processus d'embauche appropriés.

Cela implique une sélection minutieuse, une vérification rigoureuse des références, ainsi qu'une confirmation des antécédents. On conseille également de faire certains contrôles supplémentaires dans le cas où la personne embauchée doit être autorisée à effectuer des opérations financières pour le compte de l'entreprise..

Gérez efficacement les départs.

Lorsqu'un employé quitte l'entreprise, désactivez ses accès internes et en ligne. Assurez-vous que l'ex-employé ne pourra plus – de chez lui – accéder à son compte de courriel d'entreprise ou à des données de l'entreprise.

Faites un suivi périodique auprès du supérieur immédiat de vos employés.

Les fonctions d'une personne peuvent évoluer au fil du temps. Une simple question pourrait vous permettre de juger du niveau d'autorisation nécessaire à quelqu'un – par exemple : « Est-ce que Christine a encore besoin de faire des télévirements ? »

Gérez rigoureusement les limites financières.

En matière de limites d'accès (touchant, par exemple, les virements, les factures dont un employé peut

autoriser le paiement ou les chèques qu'un employé peut faire), bon nombre de propriétaires d'entreprise se contentent d'attribuer à chacun les limites maximales – d'où le nombre beaucoup trop élevé d'employés subalternes autorisés à virer des sommes considérables. Établissez les limites de chacun en tenant compte de son rang et des besoins de l'entreprise, et réévaluez-les régulièrement.

Assurez-vous que les accès des personnes qui ont quitté l'entreprise sont révoqués.

Si votre entreprise est en croissance rapide ou si certains employés travaillent à distance, il peut être difficile de rester au fait des mouvements de personnel. Pour vous assurer que seuls vos employés actifs ont accès à vos données, vérifiez si les personnes qui ont un compte d'utilisateur en vigueur figurent sur une liste à jour du personnel.

Divisez les fonctions donnant accès aux fonds de l'entreprise.

If you own a retail business, make each employee responsible for their own cash drawer so there's less opportunity to hide a theft. It's also a good idea to separate cash responsibilities: for instance, the employee who is responsible for reconciling receipts shouldn't also handle or receive cash.

CONSEIL

Prenez l'habitude de ne jamais laisser une entière latitude à un employé, même si vous lui faites implicite-ment confiance

Faites autoriser chaque opération par au moins deux personnes.

L'une des meilleures façons de lutter contre la fraude interne est de mettre en place une politique de double contrôle des opérations financières. Trop souvent, l'auteur d'un vol interne est un commis comptable ou un commis aux comptes fournisseurs – ou même un chef des finances – qui peut déplacer des fonds à sa guise sans avoir de comptes à rendre. Prenez l'habitude de ne jamais laisser une entière latitude à un employé, même si vous lui faites implicitement confiance. Et si certains de vos employés expriment du mécontentement à l'égard des contrôles que vous mettez en place, rappelez-leur qu'ils seront eux-mêmes protégés par votre politique de double contrôle si jamais ils commettent une erreur ou que leur ordinateur est infecté par un virus – car il sera possible de déceler l'erreur avant qu'elle ne devienne coûteuse pour l'entreprise.

Si vous êtes victime de fraude, signalez-le.

Souvent, les chefs d'entreprise sont gênés de signaler une fraude interne, car ils se reprochent de ne pas avoir su voir ce qui se passait dans leur entreprise. Or, il faut garder à l'esprit que les fraudeurs sont habiles, rusés et manipulateurs, et donc qu'il est souvent difficile de déceler leurs intentions malveillantes ou leurs agissements. Le fait de signaler une fraude pourrait vous aider à récupérer ce que vous avez perdu – ou, à tout le moins, éviter à d'autres entreprises d'embaucher le même escroc.

Toute entreprise, ou presque, peut être un jour victime d'une fraude interne. La meilleure façon de protéger la vôtre est d'adopter un mode de fonctionnement rigoureux en misant sur des contrôles et des politiques qui rendent le vol pratiquement impossible.

Dix conseils

pour protéger votre entreprise contre la fraude

Une entreprise peut être victime de nombreux types de fraude, allant du cybercrime au vol interne, en passant par la fraude sur paiement et le piratage psychologique. Mais si les méthodes des fraudeurs varient, les mesures à prendre pour protéger une entreprise changent peu.

Voici dix conseils qui vous aideront à protéger votre entreprise contre la fraude :

1 Soyez méfiant.

Si vous remarquez quelque chose d'étrange ou qui sort de l'ordinaire de quelque façon que ce soit, redoublez de prudence. N'ouvrez aucun courriel ou lien suspect provenant d'entreprises ou de personnes que vous ne reconnaissez pas. Faites preuve de la même méfiance à l'égard des fenêtres contextuelles et des sites Web auxquels vous accédez. Et gardez à l'esprit que si quelque chose vous semble trop beau pour être vrai, c'est probablement le cas.

2 Prenez le téléphone.

Si vous ou l'un de vos employés recevez un courriel suspect vous demandant des renseignements personnels ou concernant votre entreprise, téléphonez afin de vérifier si la demande est légitime. Et ne vous fiez jamais au fait qu'un tel courriel ou message texte contient un numéro de téléphone connu. Même si le numéro est celui de l'un de vos fournisseurs, ou encore un numéro connu d'une banque ou d'une autre entreprise, il est important de parler à quelqu'un afin de vous assurer que le courriel est légitime. Rappelez-vous : votre institution financière ne se servira jamais d'un courriel pour vous demander des renseignements personnels ou confidentiels.

3 Connaissez votre réseau.

Le courrier électronique ne doit pas être votre seul moyen de communication avec vos fournisseurs et vos collaborateurs ; ayez d'autres formes de contact avec eux, même si leur lieu de travail est loin du vôtre. Sachez reconnaître la voix et la façon d'écrire de chacun, et soyez au courant de son horaire et des politiques auxquelles il se conforme. Ainsi, si vous recevez une demande qui ne cadre pas avec les habitudes d'un fournisseur, vous vous en rendrez compte tout de suite. Vous vous sentirez également plus à l'aise de prendre le téléphone pour faire une vérification s'il y a lieu.

4 Gérez judicieusement les limites applicables aux paiements de factures et autres paiements.

Les limites (sommes pouvant être envoyées, autorisées ou versées par l'employé) attribuées aux employés ayant peu d'expérience devraient être moins élevées. Même si vous êtes occupé, ne cherchez pas à vous éviter du travail en attribuant à vos employés des limites élevées. Attribuez les limites financières appropriées et réévaluez-les régulièrement.

5 Établissez des niveaux d'approbation doubles pour les paiements.

Exigez que tous les paiements soient autorisés par au moins deux personnes – de façon à ce que l'autorité liée à ces opérations ne repose pas sur un seul individu. Ce mécanisme d'approbation à deux niveaux protégera votre entreprise. Le regard d'une deuxième personne permet de repérer des erreurs d'inattention – ou des intentions malveillantes – qui peuvent coûter cher aux entreprises.

6 Mettez à jour vos logiciels et votre navigateur.

Les logiciels qui ne sont pas à jour ne peuvent pas protéger convenablement l'information. Pour protéger votre entreprise contre les cybercriminels, installez un antivirus (et mettez-le à jour régulièrement), créez des copies de sécurité et faites appel à des spécialistes externes de la technologie. Ces mesures vous assureront également que l'entreprise pourra reprendre rapidement ses activités si jamais l'un de ses systèmes était compromis.

7 Assurez-vous.

Une attaque par rançongiciel pourrait paralyser votre entreprise et l'empêcher de fonctionner normalement durant une période indéterminée (il faut parfois des mois pour se remettre d'une telle attaque). Une assurance continuité des activités protégera votre gagne-pain et celui de vos employés si l'entreprise n'est pas en mesure de poursuivre ses activités.

8 Informez vos employés.

Assurez-vous que vos employés connaissent les menaces qui existent à l'heure actuelle et les tactiques des fraudeurs. Offrez-leur une formation portant sur les techniques et les politiques de lutte antifraude. Envisagez la possibilité de soumettre des employés choisis au hasard à une fausse attaque d'hameçonnage – afin de vérifier l'application des politiques en place. Au moyen de communications et de séances d'information périodiques, rappelez aux employés l'importance d'être vigilants. Ces rappels sont un moyen très efficace de prévenir la fraude..

9 Vérifiez régulièrement vos comptes.

Si vous suivez de près l'activité de vos comptes bancaires, toute opération frauduleuse attirera immédiatement votre attention. Gardez à l'esprit que même si votre institution financière a comme politique de rembourser toute somme liée à une opération non autorisée, elle fixe peut-être un délai pour le signalement des incidents. Si vous soupçonnez une fraude, avisez immédiatement votre banque.

10 Avisez votre service des TI si vous soupçonnez une cyberattaque.

L'équipe TI pourrait être en mesure de neutraliser une attaque contre vos systèmes, surtout si vous l'avisez immédiatement. Même si certains dommages ont pu être causés dans le cas où un employé a cliqué sur un lien malveillant, votre équipe technique pourrait limiter les effets de l'attaque sur le reste de l'entreprise.

Suivez de près l'information relative à la protection des renseignements personnels, à la fraude et aux autres questions importantes en matière de sécurité. Comme point de départ, nous vous suggérons de lire les Avis publiés par RBC ou de consulter le site du Centre antifraude du Canada.

Vous avez travaillé très fort pour bâtir votre entreprise, et vous devez maintenant travailler tout aussi fort pour la protéger, mais vous n'avez pas à le faire seul. Vous devez, entre autres, surveiller la trésorerie de votre entreprise.

Rendez-vous à la page Entreprises du site Web de RBC pour savoir comment nous pouvons vous aider à faire le suivi de vos comptes pour que vous sachiez toujours où en est votre trésorerie.

Rendez-vous sur le portail Découverte et apprentissage pour d'autres articles intéressants
decouverte.rbcbanqueroyale.com/entreprises/

Sources:
1. Center for Strategic and International Studies, Net Losses :
Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II
2-3. 2016 AFP Payments Fraud and Control Survey, Association for Financial Professionals