Prévention de la fraude Outil de gestion

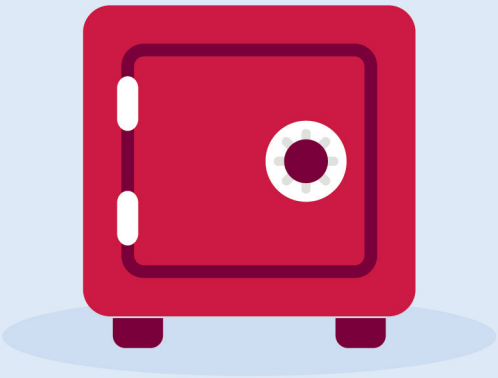
Guide sur les types courants de fraude dont sont victimes les PME

Dans cet outil de gestion, vous trouverez ce qui suit :

Renseignements généraux sur les fraudes

Que vous soyez propriétaire, gestionnaire ou employé, une chose est sûre : vous travaillez fort pour votre entreprise. Il doit en être de même pour vos systèmes de cybersécurité et vos mesures de prévention de la fraude.

Lorsque tout le monde s'engagera activement à reconnaître et à empêcher la fraude, votre entreprise sera mieux protégée contre les cybercriminels.



Piratage psychologique

Recours à la psychologie pour manipuler l'instinct humain et susciter une réaction aux demandes urgentes et à la peur afin d'amener les victimes à divulguer des renseignements confidentiels qui pourraient être utilisés pour commettre une fraude financière.

Fondement de nombreuses escroqueries

Les fraudeurs utilisent des tactiques de **piratage psychologique** pour obtenir des renseignements confidentiels sur leurs victimes et en tirer profit. Ces tactiques prennent souvent la forme de courriels, d'appels et de messages textes suspects qui peuvent sembler provenir de membres de la famille, de clients, de fournisseurs ou d'autres employés. Une fois obtenus, les renseignements seront utilisés pour commettre une fraude financière et épuiser les fonds de la victime.

Voici trois principales caractéristiques des techniques de piratage psychologique :

Utilisation de la peur comme facteur de motivation en envoyant des courriels, des appels téléphoniques ou des messages textes menaçants pour vous inciter à divulguer des renseignements ou à effectuer des opérations

Demandes urgentes et imprévues de renseignements personnels ou de renseignements sur l'entreprise au moyen de communications écrites comme des courriels ou des messages textes

Offres, prix ou concours qui semblent trop beaux pour être vrais et qui prétendent souvent offrir une récompense en échange de renseignements de connexion ou d'autres renseignements personnels ou sur l'entreprise

Types d'escroqueries dont votre entreprise pourrait être la cible

1. Stratagème de compromission des courriels d'affaires

Dans le contexte du stratagème de compromission des courriels d'affaires, les **fraudeurs exploitent les employés d'entreprises qui ont le pouvoir d'effectuer des opérations commerciales** en se faisant passer pour un fournisseur ou un employé connu. Les fraudeurs peuvent réussir à s'approprier le courriel authentique du fournisseur ou créer un compte de courriel très semblable, puis communiquer avec votre entreprise pour demander des paiements de services ou de produits vers un compte qui leur appartient. Les deux formes les plus courantes du stratagème de compromission des courriels d'affaires sont l'escroquerie du chef de la direction et du cadre supérieur, dans le contexte desquelles le fraudeur se fait passer pour un cadre supérieur de l'entreprise et demande des renseignements personnels ou un virement de fonds dans un compte, ainsi que les fraudes liées aux factures, décrites ci-dessous.

2. Fraudes liées à de fausses factures

Forme de stratagème de compromission des courriels d'affaires, les fraudes liées aux factures comportent deux volets : le fraudeur peut se présenter comme un fournisseur connu qui **demande à votre entreprise de fournir des renseignements de facturation à jour** ou demander un paiement pour une facture à venir qui **ne correspond pas aux cycles de facturation habituels de votre entreprise**. Ignorant qu'il s'agit d'une fraude, vos employés remettent les fonds au fraudeur, ce qui donne souvent lieu à des fonds irrévocables dont votre entreprise est tenue responsable.

3. Rançongiciels

Dans les cas de fraude par rançongiciel, un **logiciel malveillant (maliciel) est installé sur votre ordinateur**, ce qui permet à un fraudeur de verrouiller à distance vos fichiers importants et d'y empêcher l'accès. Les données peuvent aussi être extraites et utilisées ultérieurement à d'autres fins frauduleuses. Les victimes de cette escroquerie recevront souvent des messages contextuels indiquant que les fichiers sont verrouillés et **exigeant le paiement d'une rançon** par l'envoi de fonds non retraçables dans le compte du fraudeur afin de récupérer l'accès aux documents.

Remarque : un rançongiciel est souvent installé sur un ordinateur lorsque la victime clique sur un lien suspect dans un courriel d'hameçonnage ou une fenêtre contextuelle d'un site Web suspect. Dans certains cas, la victime peut être appelée à télécharger un fichier intégré, ce qui masque un téléchargement de logiciel.

4. Fraudes de commerçants

Dans le contexte d'une fraude de commerçant, les fraudeurs se dissimulent sous une entité légitime en **prétendant offrir des échantillons de produits gratuits ou vendre des produits qu'ils n'ont pas**. Ils peuvent téléphoner ou envoyer un courriel à votre entreprise pour demander un virement télégraphique, des renseignements sur votre carte de crédit et une adresse avant d'expédier la marchandise. **Une fois que les fonds ou les renseignements confidentiels ont été envoyés au fraudeur, celui-ci cesse de communiquer avec vous** et n'expédie pas les produits annoncés. De nombreuses PME ont été victimes de fraudes de commerçants, en particulier pendant la pandémie de COVID-19, les fraudeurs prétendant vendre des masques en échange de fonds.

Cinq pratiques exemplaires que vous pouvez mettre en œuvre dès maintenant pour protéger votre entreprise contre la fraude

1. Vérifiez les instructions de paiement reçues par courriel ou par téléphone

Examinez toujours les instructions de paiement et les demandes de modification des renseignements de paiement d'un compte avec scepticisme, que ce soit par courriel ou par téléphone. Assurez-vous que vos employés communiquent avec un représentant connu de votre ou de vos fournisseurs à qui ils ont déjà parlé en utilisant un numéro de téléphone figurant au dossier. Vous pourriez aussi envisager de coordonner un mode de confirmation des renseignements sur le mode de paiement en personne par l'intermédiaire de Microsoft Teams, de Skype ou d'autres technologies sécurisées.

2. Renseignez vos employés sur la fraude et sur les procédures Connaître votre clientèle (CVC)

Renseignez vos employés sur la cybercriminalité et les tendances en matière de fraude afin qu'ils puissent faire la distinction entre les communications réelles et fictives. En outre, donnez-leur les moyens de mettre en pratique les procédures Connaître votre clientèle (CVC) dans le cadre de leurs activités. Voici quelques exemples :

- Comprendre qui sont les clients de votre entreprise et si les courriels ou les demandes provenant d'eux sont logiques
- Suivre un processus de vérification des appels téléphoniques comprenant des numéros de téléphone fiables entre votre conseiller PME CIBC et les clients afin que les opérations puissent être vérifiées et que les activités suspectes fassent l'objet d'une enquête

3. Confirmez que vos systèmes de cybersécurité sont solides et à jour

Exécutez régulièrement des analyses de système sur vos ordinateurs à l'aide d'un logiciel antivirus pour détecter et supprimer les logiciels malveillants de vos appareils et utilisez un pare-feu pour bloquer l'accès non autorisé aux réseaux de votre entreprise. Effectuez vos recherches pour vous assurer d'utiliser des systèmes d'exploitation et de cybersécurité à jour. Sauvegardez les renseignements de votre entreprise dans un nuage sécurisé ou un autre logiciel de sauvegarde pour les protéger contre les rançongiciels et cyberattaques qui pourraient toucher votre ordinateur.

4. Ralentissez. N'agissez pas trop vite.

Les fraudeurs sont exigeants et veulent que vous agissiez rapidement. Gardez la maîtrise de toute situation en ralentissant; réfléchissez attentivement à ce qu'on vous demande et déterminez si cela vous paraît logique. Menez une enquête sur les demandes de renseignements personnels et vérifiez leur légitimité avant de les communiquer.

5. Établissez de solides contrôles internes pour déterminer qui administre les données de votre entreprise

Il est important de limiter les autorisations et le traitement des données confidentielles à des personnes désignées, surtout dans une PME. Déployez des mesures de contrôles comme les suivantes :

- Restreindre l'accès des employés aux données financières, aux dossiers informatiques et aux stocks
- Utiliser les pistes de vérification pour faire le suivi de toutes les opérations financières et les vérifier régulièrement
- Mettre en vigueur un processus d'approbation par plusieurs personnes pour les demandes de remboursement de dépenses, les heures supplémentaires, le tirage de chèques et les activités liées à la paie

Connaître votre fraude avant qu'il ne soit trop tard

Veuillez communiquer immédiatement avec la Banque CIBC au 1 800 465-2422 si vous croyez avoir été victime d'une fraude, si vos comptes d'entreprise ont été compromis ou si votre identité a été volée.

Protéger votre entreprise

Pour prévenir la fraude, vous devez être proactif, renseigner vos employés sur les risques auxquels ils peuvent être exposés et être au courant de tous les documents, de toutes les activités en ligne et de tous les achats de votre entreprise. La mise en œuvre d'un plan de prévention de la fraude et de cybersécurité peut aider votre entreprise à mieux se préparer pour éviter une fraude financière.

Autres ressources

Centre antifraude du Canada :
centreantifraude.ca

Better Business Bureau (BBB) Scam
Outil de suivi et conseils sur la fraude :

BBB.org/ScamTracker
BBB.org/ScamTips

Bureau de la concurrence Canada :
bureaudelaconcurrence.gc.ca

Gendarmerie royale du Canada :
RCMP-GRC.gc.ca/fr

Pour en savoir plus sur les services bancaires aux entreprises, visitez le site cibc.com/entreprise