TYPES DE FRAUDE QUI PEUVENT AVOIR UNE INCIDENCE SUR VOTRE ENTREPRISE

Prévention de la fraude

Compromission des courriels de clients

La compromission des courriels de clients a lieu lorsqu'un fraudeur accède au compte de courriel d'un utilisateur et obtient des informations sur ses interactions avec la banque et avec d'autres contacts. Le fraudeur se fait ensuite passer pour le client en utilisant le compte de courriel du client ou en créant un compte qui y ressemble. Cet accès est ensuite utilisé pour envoyer des demandes aux institutions financières ou à d'autres contacts de l'utilisateur, demander des modifications à l'accès bancaire et envoyer des instructions de paiement dans le but d'exfiltrer des fonds.

Compromission des courriels d'entreprise

La compromission des courriels d'entreprise a lieu lorsqu'un fraudeur se fait passer pour une personne connue et en qui sa victime a confiance, comme un fournisseur ou un dirigeant d'entreprise. Le fraudeur utilise ensuite cette relation pour tromper la victime en lui extirpant des renseignements clés qu'il utilisera plus tard à des fins de détournement de fonds. La fraude se termine par une demande de fonds qui semble urgente et qui, sans vérification adéquate, seront envoyés à la destination frauduleuse.

Les criminels peuvent communiquer avec une entreprise par téléphone, par courriel ou par message texte et se faire passer pour un gouvernement, une entreprise ou un service essentiel, tels que :

- Une institution financière, comme Visa ou Mastercard, demandant des renseignements bancaires
- Une agence de santé publique, comme Santé Canada, l'Organisation mondiale de la santé ou un hôpital local, demandant des renseignements personnels
- L'ARC ou un organisme d'application de la loi qui exige un paiement immédiat sous forme de cryptomonnaies, comme du bitcoin, des cartes-cadeaux ou tout service d'envoi de fonds, comme un Virement de fonds mondial CIBC ou un virement télégraphique
- Une société de services publics ou un fournisseur de services demandant un paiement de fonds en raison d'un retard ou de frais non facturés

Rançongiciels

Les rançongiciels sont couramment envoyés aux victimes par l'intermédiaire de sites Web et de courriels malveillants. Les canaux de médias sociaux peuvent aussi être un point d'entrée pour les acteurs mal intentionnés. Le rançongiciel est essentiellement un virus informatique qui fait une copie de fichiers critiques sur les ordinateurs ou serveurs connectés d'une victime sur le réseau. Les fichiers sont ensuite envoyés au fraudeur, puis le virus chiffre tous les fichiers originaux dans le réseau. Une fois que le virus aura chiffré les renseignements, le fraudeur communiquera avec la victime pour demander une rançon en échange du déchiffrement des fichiers et s'engagera à ne pas utiliser ni divulguer les renseignements volés. Les fraudeurs peuvent aussi vendre les données qu'ils ont obtenues lors d'une attaque par rançongiciel à d'autres fraudeurs afin qu'elles puissent être utilisées à l'avenir.

Signaler la fraude et les arnaques

Avez-vous déjà été témoin de ces signes de fraude?

Signalez immédiatement toute activité suspecte à votre directeur relationnel ou à la ligne de signalement de fraude du Centre de services affaires CIBC : 1-800-500-6316

ou consultez la Politique de la Banque CIBC sur la protection des renseignements personnels sur le site CIBC.com/francais

Mesures de prévention et pratiques exemplaires

La prévention de la fraude consiste à être proactif. La mise en œuvre d'un plan de prévention de la fraude et de cybersécurité peut aider votre organisation à mieux se préparer pour éviter une fraude financière. De nos jours, les criminels ciblent des organisations pour divers types de fraude, sachant que bon nombre d'entre elles sont de plus en plus vulnérables. Se tenir informé est la première ligne de défense pour éviter d'être victime d'une fraude. Les mesures de prévention et pratiques exemplaires ci-dessous limiteront le risque de fraude en ce qui concerne les tentatives de fraude courantes.

- Confirmez verbalement les instructions de paiement, surtout si des modifications sont apportées aux directives de paie des employés et aux paiements des fournisseurs. Assurez-vous d'utiliser un numéro de téléphone inchangé connu et évitez d'utiliser les coordonnées contenues dans la demande elle-même.
- Habituellement, on ne vous demandera pas de fournir des renseignements bancaires ou personnels. Faites attention aux personnes avec qui vous communiquez vos renseignements personnels, comme votre numéro d'assurance sociale (NAS) ou vos renseignements bancaires.
- Ne divulguez jamais vos NIP ou mots de passe à quiconque.
- Modifiez souvent vos mots de passe et assurez-vous d'utiliser des mots de passe solides combinant des majuscules, des chiffres et des caractères spéciaux.
- Méfiez-vous des gestionnaires de mots de passe.
- Établissez des contrôles d'accès fondés sur les rôles et l'approbation double des paiements.
- Utilisez l'authentification multifactorielle dans la mesure du possible.
- Mettez en œuvre les contrôles d'enregistrement du système.
- Faites le rapprochement des comptes bancaires et la correction des écarts en temps opportun. Communiquez immédiatement avec le Centre de services aux entreprises CIBC pour toute opération (paiement par câble, TLV, chèque) que vous jugez inhabituelle ou inconnue.
- Protégez les formules de chèque et éliminez les enveloppes « à fenêtre » pour poster des chèques.
- Pour la plupart des victimes d'une attaque de rançongiciel, il est essentiel d'avoir une copie de sauvegarde des fichiers physiquement déconnectée du réseau.
- Gardez vos logiciels, y compris vos systèmes d'exploitation et vos applications, à jour. Utilisez un logiciel antivirus ou un anti-maliciel.
- Méfiez-vous des demandes et des écrans inconnus qui s'affichent dans tout site Web ou toute application que vous utilisez couramment.
- Mettez en place des mesures de détection des compromissions et mettez au point un plan d'intervention en cas d'incident de cybersécurité.
- Réfléchissez avant de cliquer! N'ouvrez pas de pièces jointes ou ne cliquez pas sur des liens intégrés à des courriels en provenance d'expéditeurs inconnus.

Ces conseils sont fournis uniquement à titre informatif. Pour obtenir des conseils sur mesure pour votre organisation, veuillez vous adresser à des experts de la prévention de la fraude.

Cyberassurance

Une fois que vous avez pris les mesures préventives nécessaires et appliqué les pratiques exemplaires pour protéger votre entreprise contre les cyberattaques, la cyberassurance peut aussi être considérée comme une mesure de protection supplémentaire. Il existe de nombreuses variantes et de nombreux types de cyberassurance, qui peuvent être très personnalisables et comporter de multiples facettes. Pour en savoir plus sur la cyberassurance, visitez le site du Bureau d'assurance du Canada.

Discutez avec votre courtier d'assurance des types de cyberassurance et de couverture spécifiques qui conviennent à votre entreprise.