Northbridge Assurance | CYBERSCOUT A TransUnion® Brand

PARLONS PRÉVENTION

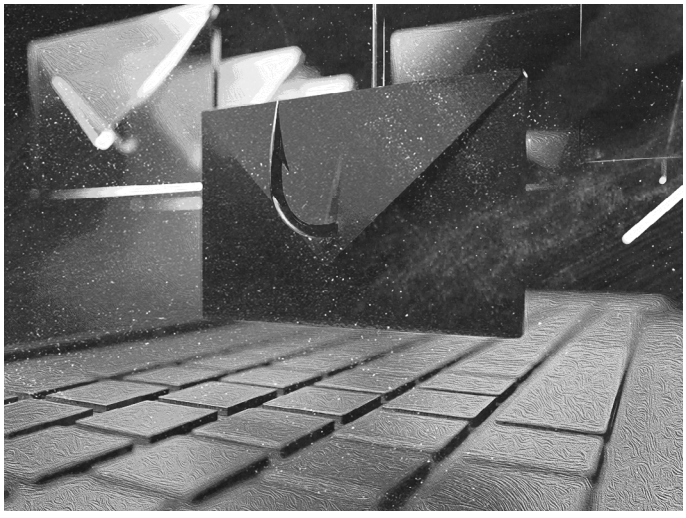
FRAUDE PAR COURRIEL D'AFFAIRES COMPROMIS : CONSEILS POUR ÉVITER LES PIÈGES

Vous connaissez le dicton : « Il ne faut jamais ouvrir le courriel d'une personne que vous ne connaissez pas ». Vous présumez que vos employés savent reconnaître l'hameçonnage et qu'ils ne cliqueront pas sur des hyperliens suspects ou n'ouvriront pas de pièce jointe de provenance inconnue.

Mais que se passe-t-il s'ils reçoivent un courriel qui semble provenir de votre conseiller financier, d'un fournisseur de confiance ou même de vous?

Les cybercriminels qui cherchent à soutirer de l'argent et des renseignements personnels aux entreprises se tournent de plus en plus vers la fraude par courriels d'affaires compromis. Ils ciblent les entreprises qui utilisent des virements électroniques et celles qui dépendent de fournisseurs étrangers et de vendeurs ou de clients tiers. L'usurpation de l'identité de ces partenaires commerciaux de confiance rend la fraude par courriel d'affaires compromis pratiquement impossible à détecter et très difficile à gérer une fois que le mal est fait.

Selon des statistiques récentes sur la cybercriminalité, le harponnage, qui comprend la fraude par courriel d'affaires compromis, continue d'être l'une des fraudes les plus signalées parmi les quelque 40 types enregistrés par le Centre antifraude du Canada (CAFC). En 2020, les signalements au CAFC pour ce type de fraude représentaient des pertes de près de 30 millions de dollars, et au premier trimestre de 2021 seulement, plus de 26 millions de dollars en pertes ont été signalés.



QUATRE MÉTHODES DE FRAUDE PAR COURRIEL D'AFFAIRES COMPROMIS

La difficulté de détecter la fraude par courriel d'affaires compromis réside dans la manière dont les escrocs utilisent des relations professionnelles existantes pour accéder aux fonds ou aux renseignements personnels d'une entreprise. Les criminels utilisent les courriels d'affaires compromis pour réaliser quatre types de fraudes spécifiques.

Méthode 1 : fraude du président

Le courriel du président de l'entreprise est piraté ou imité
L'imposteur contacte le service des finances pour demander un virement.

Le service des finances autorise le virement
Le courriel de demande indique généralement que le virement doit être effectué rapidement et discrètement.

Les fonds sont déposés dans le compte du fraudeur
Le virement est effectué vers le compte bancaire frauduleux du criminel.

Les escrocs utilisent l'adresse courriel d'un haut dirigeant pour contacter un employé responsable des finances de votre entreprise et lui demander d'effectuer un virement important vers des comptes bancaires frauduleux. Étant donné que la plupart des entreprises utilisent le courriel comme principal moyen de communication entre les employés et les services, ce type de fraude est presque toujours détecté après le virement.

Méthode 2 : fraude à la fausse facture

Le courriel d'un employé est piraté ou imité
L'imposteur envoie des courriels par l'intermédiaire d'un compte compromis aux fournisseurs et aux clients de l'entreprise pour demander le paiement de fausses factures.

Les clients et les fournisseurs paient les fausses factures
Les courriels de demande indiquent généralement des factures « nouvelles » ou « modifiées ».

Les fonds sont déposés dans le compte du fraudeur
Le virement est effectué vers le compte bancaire frauduleux du criminel.

La deuxième méthode vise vos clients ou des fournisseurs tiers. Les fraudeurs espèrent obtenir de l'argent en demandant le paiement de fausses factures. Ils peuvent pirater les courriels de vos employés et envoyer des factures urgentes, à l'instar de la méthode utilisée avec les fournisseurs étrangers.

Méthode 3 : fraude au faux fournisseur

La troisième méthode vise les fournisseurs ou vendeurs étrangers d'une entreprise. Les malfaiteurs espèrent obtenir l'autorisation d'effectuer des virements vers un compte frauduleux. Les criminels piratent le courriel d'un fournisseur et demandent un virement vers un « nouveau » compte, en prétendant que le fournisseur à l'étranger a déménagé ou changé d'adresse.

Méthode 4 : fraude par demande de renseignements personnels

Le courriel des ressources humaines est piraté ou imité.
L'imposteur utilise un compte compromis pour demander des renseignements personnels.

Les employés envoient des documents confidentiels ou remplissent des formulaires frauduleux en ligne
En général, les courriels de demande indiqueront que les renseignements n'ont jamais été recueillis, qu'ils ont été perdus ou qu'ils doivent être mis à jour.

Le fraudeur obtient des renseignements personnels
Les renseignements permettant d'identifier des personnes peuvent être utilisés pour voler des identités ou vendus sur le marché noir.

Contrairement aux trois premières méthodes, cette dernière méthode se concentre sur le vol de renseignements personnels d'employés. Les fraudeurs ciblent les comptes de courriel des ressources humaines pour obtenir des renseignements permettant d'identifier des personnes. Des courriels sont envoyés depuis le compte piraté d'un membre des ressources humaines à d'autres employés, leur demandant de fournir ou de vérifier des renseignements confidentiels.

CONSEILS POUR PROTÉGER VOTRE ENTREPRISE

La fraude par courriel d'affaires compromis peut comporter de nombreux niveaux de compromission potentielle et entraîner des répercussions sur toutes les personnes associées à une entreprise. En suivant ces conseils, vous pouvez contribuer à vous tenir au courant, vous, vos employés et vos fournisseurs, sur les fraudes par courriels et autres escroqueries visant les entreprises :

1. **Élaborez et mettez en œuvre un programme de sensibilisation à la sécurité à l'échelle de l'entreprise**
   Faites de la protection des renseignements de l'entreprise l'affaire de tous.
2. **Ne vous fiez pas uniquement au courriel pour effectuer des virements**
   Confirmez les demandes de virement de fonds en procédant à des vérifications par téléphone ou en organisant des réunions en face à face. Utilisez des numéros de téléphone connus pour valider l'authenticité des demandes de virement et faites une vérification en personne chaque fois que cela est possible.
3. **Examinez attentivement toutes les demandes de virement de fonds envoyées par courriel**
   Vérifiez que les adresses courriel ne contiennent aucune variation qui sorte de l'ordinaire.
4. **Renforcez la sécurité de vos réseaux, surtout en ce qui concerne les appareils mobiles**
   Parmi les menaces qui guettent les appareils mobiles, citons les logiciels espions, les connexions sans fil non sécurisées et même les faux réseaux. Comme il arrive que les employés utilisent des appareils mobiles personnels pour effectuer des tâches professionnelles, notamment consulter leurs courriels, les cybercriminels les ciblent souvent pour créer des passerelles vers votre réseau.

Pour savoir comment mieux protéger votre entreprise, communiquez avec votre courtier d'assurance ou rendez-vous au **www.northbridgeassurance.ca**.

[4040-001-ed03F | 05.2023]

Northbridge Assurance | CYBERSCOUT A TransUnion® Brand