GRC
GENDARMERIE ROYALE DU CANADA

BULLETIN
COURRIELS D'AFFAIRES COMPROMIS

Reconnaissez-les, rejetez-les et signalez-les!

Selon des statistiques récentes sur la cybercriminalité, les courriels d'affaires compromis sont à l'origine de vols totalisant plus de ***5 milliards de dollars*** *auprès de victimes sans méfiance du monde entier, y compris des entrepreneurs canadiens[i]. Selon le Centre anti-fraude du Canada (CAFC), il s'agit de la deuxième fraude en importance pour les pertes monétaires sur plus de quarante types de fraudes répertoriés. Cette fraude est réelle et en plein essor, mais elle peut être prévenue grâce à une sensibilisation accrue.*

Bulletin 3. Version 1.0
mars 2018

RECONNAISSEZ-LES!

Que sont les courriels d'affaires compromis?

Le courriel d'affaires compromis, aussi appelé fraude au président, fraude par virement bancaire ou arnaque des dirigeants d'entreprise, il s'agit d'une ruse complexe qui trompe une entreprise en lui faisant verser une somme d'argent à un fraudeur. Ce stratagème est réalisé à l'aide de techniques d'ingénierie sociale[1] ou de techniques d'intrusion informatique. Plusieurs types de stratagèmes impliquant des courriels d'affaires compromis ont été observés au Canada :

- **Stratagème 1 :** Implique des comptes de courriel usurpés[2] ou compromis[3] appartenant à de hauts dirigeants. Un courriel est envoyé depuis ces comptes à un autre employé, souvent une personne chargée des transactions financières de l'entreprise, dans le but de demander un virement bancaire pour une raison qui semble valable sur le plan opérationnel.
- **Stratagème 2 :** Implique des entreprises qui ont des relations bien établies avec des fournisseurs. Le fraudeur utilise un compte de courriel usurpé ou compromis de l'entreprise pour demander au fournisseur d'effectuer un virement bancaire dans un compte frauduleux.
- **Autres stratagèmes :** Peuvent inclure des demandes de données comme des renseignements fiscaux qui seront utilisés ultérieurement pour mener des activités frauduleuses; des demandes de paiements de factures « légitimes » qui se révéleront fausses lorsque le vrai fournisseur appellera pour demander l'état des paiements des factures; et des malfaiteurs qui communiquent avec des entreprises et se font passer pour des avocats traitant des dossiers confidentiels ou urgents. Il existe d'autres variations de ces stratagèmes impliquant des courriels d'affaires compromis, en fait, de nouvelles ruses sont élaborées régulièrement.

REJETEZ-LES!

Comment puis-je protéger mon entreprise?

- Mettre l'accent sur l'éducation et la prévention pour les employés en les formant sur les bonnes pratiques de sécurité.
- Méfiez-vous des courriels d'apparence légitime, mais non sollicités vous demandant de procéder à des virements bancaires et vous pressant d'agir rapidement ou confidentiellement.
- Examinez attentivement l'adresse du courriel – elle pourrait ressembler à une adresse légitime, mais être légèrement différente. P. ex. : si l'adresse réelle était abc-123@mail.ca, l'adresse usurpée pourrait être abc_123@mail.ca ou abc123@mail.ca.
- Créer des règles de système de détection d'intrusion qui mettent en évidence les courriels dont l'extension est semblable à celle de l'entreprise et enregistrer toutes les variantes du nom de domaine Internet de l'entreprise.[4]
- Envisagez un processus de vérification des virements bancaires en deux étapes. Communiquez avec la source par un moyen de communication différent (p. ex. par téléphone) pour confirmer la légitimité de la demande. Ne vous fiez pas uniquement aux courriels.
- Mettez en œuvre un système à deux signatures avec authentification mutuelle (utilisation d'un jeton de sécurité) exigeant la signature d'au moins deux employés autorisés pour les virements bancaires.
- Méfiez-vous des courriels mal rédigés incluant des erreurs grammaticales évidentes ou des tournures maladroites qui ne sont pas couramment utilisées au Canada. Cependant, les arnaques plus complexes incluront le langage et la grammaire utilisés dans votre correspondance quotidienne.
- Surveillez les habitudes de vos clients, y compris les raisons, les détails et les montants des paiements. Soyez à l'affût de tout changement important.
- N'ouvrez jamais les courriels ou les pièces jointes provenant d'adresses inconnues, car ils peuvent contenir des logiciels malveillants (maliciels) utilisés pour compromettre les comptes courriel.
- Amorcez une nouvelle chaîne de courriels au lieu de répondre directement à un courriel de demande de virement bancaire.
- Limitez la diffusion de renseignements sur le personnel et les finances de l'entreprise dans les médias sociaux et les sites Web, y compris les absences du PDG ou du directeur financier, ainsi que les noms et les titres des agents financiers. Les fraudeurs utiliseront ces renseignements pour mener des recherches, planifier le moment de leur attaque et choisir des cibles futures.
- Veillez à ce que tous les logiciels, y compris les logiciels antivirus, soient à jour sur tous les ordinateurs, les serveurs et les appareils, notamment les téléphones cellulaires et les tablettes.

Autres mesures

- Évitez d'utiliser des comptes courriel gratuits sur le Web pour mener les activités de votre entreprise, car ils sont plus susceptibles d'être compromis.
- Méfiez-vous d'une augmentation du nombre de courriels d'hameçonnage, car cela pourrait indiquer une future tentative de fraude par courriel d'affaires compromis. Assurez-vous que tous les employés savent qu'ils doivent signaler ces courriels au service de la cybersécurité de l'entreprise.
- Envisagez l'établissement d'une liste blanche des adresses de courriel et domaines autorisés. Les courriels provenant d'adresses inconnues peuvent être bloqués ou signalés.

1 – Recours à des manœuvres trompeuses pour mener des personnes à divulguer des renseignements confidentiels ou personnels pouvant être utilisés à des fins frauduleuses (intrusion non technique).
2 – L'usurpation de courriel est la falsification d'un en-tête de courriel pour que le message semble provenir d'une personne autre que l'expéditeur réel.
3 – Le compte courriel a été piraté. Un fraudeur a accès au compte courriel.
4 – Aussi appelée « sosie de nom de domaine », cette méthode est de plus en plus utilisée. Un sosie de nom de domaine est un nom de domaine créé et enregistré légalement par des malfaiteurs parce qu'il est presque identique au nom de domaine de l'organisation ciblée.

BULLETIN COURRIELS D'AFFAIRES COMPROMIS

SIGNALEZ-LES!

Comment mon entreprise doit-elle réagir?

1. Si le courriel est reconnu comme étant frauduleux **APRÈS** le transfert de fonds :

A) **Signalez immédiatement** l'incident à votre institution financière. Fournissez l'information suivante :

- Le montant
- Le compte destinataire
- Tout autre détail pertinent de la demande
- Informez-vous sur le rappel du transfert
- Assurez-vous que votre institution financière communique avec l'institution financière destinataire

B) **Signalez** l'incident au service de police local. Indiquez qu'il s'agit d'une fraude par courriel d'affaires compromis ou d'une fraude par virement bancaire. Ce sont là des infractions en vertu de l'article 380 (Fraude) ou de l'article 403 (Fraude à l'identité) du Code criminel. Il ne s'agit PAS d'une affaire de nature civile. Cela s'applique également aux tentatives de fraude par courriel d'affaires compromis.

Si une technique d'intrusion électronique a été tentée ou utilisée, des infractions criminelles additionnelles ont été commises, notamment en vertu de l'article 342.1 (Utilisation non autorisée d'ordinateur) ou de l'article 430 (1.1) (Méfait à l'égard de données informatiques) du Code criminel. Soyez prêt à fournir tous les détails de l'incident.

C) **Envisagez** l'élaboration d'un plan pour répondre aux demandes des médias concernant toute perte financière.

D) **Signalez** l'incident au Centre antifraude du Canada (CAFC) en ligne, à tout moment, à l'adresse http://www.antifraudcentre.ca/index-fra.htm. Veuillez cliquer sur l'onglet « Signaler un incident » et ensuite sur le lien « Système de signalement des fraudes ». Vous pouvez aussi joindre le CAFC au 1-888-495-8501, de 9 h à 16 h 45 (HNE) du lundi au vendredi.

E) **Signalez** l'incident au Centre canadien de réponse aux incidents cybernétiques (CCRIC) **par courriel** à ps.cyberincident-cyberincident.sp@canada.ca ou visitez le site https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fr.aspx. Le CCIRC aide à établir des mesures d'atténuation et de prévention, surtout dans les cas de fraude technologique. Indiquez au CCIRC si les services de police ont été prévenus.

2. Si le courriel est reconnu comme étant frauduleux **AVANT** le transfert de fonds:
   - Suivez les étapes **1B, 1D et 1E** ci-dessus.
3. Si applicable à votre entreprise:
   - Informez la haute direction et/ou le conseil d'administration de votre entreprise au sujet de l'incident, le cas échéant.
   - Menez une enquête judiciaire interne de la TI et envisagez de demander l'aide de spécialistes de la sécurité externes.
   - Enquêtez sur les violations possibles de la politique de sécurité, et élaborez un plan pour résoudre les lacunes en matière de sécurité.

Il est fortement recommandé de SIGNALER L'INCIDENT pour les raisons suivantes :

- Peu importe si des fonds ont été transférés ou non, un acte criminel a été commis. N'oubliez pas que chaque signalement est important et constitue un outil précieux pour les enquêteurs.
- Si l'arnaque n'est pas signalée, il n'y a pas de dossier sur l'incident. Par conséquent, l'envergure et la portée de cette activité frauduleuse ne peuvent pas être comprises ou faire l'objet d'une enquête.
- N'ayez pas peur ou honte de signaler l'incident. Les auteurs de ces crimes utilisent des techniques de plus en plus complexes qui peuvent même tromper les entrepreneurs les mieux informés.

Pour en savoir davantage, consultez :

Pensez cybersécurité - www.pensezcybersecurite.gc.ca

Bureau de la concurrence - http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/04201.html

Internet Crime Complaint Centre (IC3) du FBI - https://www.ic3.gov/media/2016/160614.aspx#fn1 (en anglais seulement)

Global Cyber Alliance https://www.globalcyberalliance.org (en anglais seulement)

En consultation avec :

CALGARY POLICE SERVICE

PEEL REGIONAL POLICE

i – Statistiques les plus récentes du FBI sur les courriels d'affaires compromis : https://www.ic3.gov/media/2017/170504.aspx