BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Harponnage :
Qu'ont les fraudeurs dans leurs boîtes à outils?

2023-03-14

LA FRAUDE : IDENTIFIEZ-LA, SIGNALEZ-LA, ENRAYEZ-LA

Chaque année en mars a lieu le Mois de la prévention de la fraude; à cette occasion, le CAFC lance une campagne de prévention pour informer et sensibiliser le public à l'importance de se protéger contre la fraude. Cette année, la campagne s'intitule ***Les ficelles du métier : qu'y a-t-il dans la boîte à outils d'un fraudeur?*** Suivez-nous sur les réseaux sociaux et consultez notre site Web pour obtenir de l'information sur la prévention de la fraude. N'oubliez pas d'utiliser le mot-clic #MPF2023 dans tous vos messages sur la prévention de la fraude.

Harponnage

Le harponnage est une des fraudes les plus courantes ciblant les entreprises et les organisations. Les fraudeurs prennent le temps de recueillir des renseignements sur leurs cibles afin d'envoyer des courriels convaincants qui semblent provenir d'une source fiable. Ils s'infiltrent dans le compte de courriel d'une entreprise ou d'un particulier ou le mystifient. Ils créent une règle pour envoyer une copie des courriels entrants à l'un de leurs comptes et épluchent ces courriels pour :

- étudier le niveau de langue utilisé par l'expéditeur;
- trouver des caractéristiques liées à des personnes, à des dates et à des paiements importants.

Variantes des attaques de harponnage :

- Une entreprise reçoit une copie d'une facture contenant des données de paiement à jour provenant apparemment d'un fournisseur ou d'un entrepreneur avec lequel elle fait affaire.
- Un comptable ou un planificateur financier reçoit une demande de retrait d'une somme importante qui semble provenir du compte de courriel d'un client.
- Le service de la paye reçoit un courriel semblant provenir d'un employé qui veut mettre à jour ses renseignements bancaires.
- Les membres d'une église, d'une synagogue, d'un temple ou d'une mosquée reçoivent une demande de don par courriel provenant prétendument de leur chef religieux.
- Un courriel qui semble provenir d'une source de confiance vous demande de télécharger une pièce jointe, mais celle-ci est un maliciel qui infiltre l'ensemble du réseau ou de l'infrastructure;
- Un courriel qui semble provenir d'une source de confiance vous demande d'acheter des cartes-cadeaux.

Qu'y a-t-il dans la boîte à outils d'un fraudeur?

Usurpation d'identité

- Les fraudeurs prennent le temps d'étudier comment votre entreprise ou organisation fonctionne et lorsqu'ils passent à l'action, ils semblent crédibles.

Mystification

- Le fraudeur pirate le compte d'une entreprise ou d'une organisation ou l'imite.
- En se faisant passer pour une personne d'autorité ou d'influence (p. ex. cadre supérieur, chef religieux, client, représentant des Ressources humaines, comptable, etc.), le fraudeur joue sur le fait que vous ne remettrez pas en question sa demande de virements ou de renseignements.

Prétexte de l'urgence

- Le fraudeur prétexte une urgence pour vous pousser à envoyer de l'argent ou à fournir des renseignements avant que vous ayez eu le temps de vérifier auprès d'autres personnes si la demande est légitime.

Qu'y a-t-il dans votre boîte à outils?

Temps

- Ce cédez pas à la pression des fraudeurs qui tentent de vous pousser à prendre une décision hâtive et regrettable; prenez toujours le temps de vérifier la légitimité de la demande. Validez la demande auprès de votre gestionnaire ou du service approprié. N'utilisez pas les coordonnées fournies par la personne qui fait la demande.

Instinct et raison

- Si la demande sort de l'ordinaire, faites des vérifications avant d'y répondre.
- Si vous recevez une communication d'une personne qui ne vous contacte généralement pas, comme un haut dirigeant, renseignez-vous.
- Passez le curseur de votre souris sur l'adresse courriel ou le lien fourni pour en confirmer l'exactitude.

Protection des renseignements personnels et sécurité

- Limitez la quantité d'information diffusée publiquement et faites preuve de prudence dans les médias sociaux.
- N'ouvrez pas les courriels non sollicités et ne cliquez pas sur les pièces jointes ou les liens suspects.
- Créez des mots de passe forts et mettez-les à jour régulièrement.
- Mettez régulièrement à jour votre ordinateur et votre réseau.
- Envisagez de faire certifier votre entreprise auprès de CyberSécuritaire Canada.

Procédures et bonnes pratiques

- Mettez en place des modalités de paiement détaillées.
- Exigez la vérification des demandes inhabituelles.
- Établissez des mesures de détection, de gestion et de signalement des fraudes.

Sensibilisation et formation des employés

- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez tous les employés.
- Offrez une formation sur la fraude aux nouveaux employés.

Obtenez d'autres conseils pour vous protéger contre la fraude.

Si vous pensez avoir été victime de cybercriminalité ou de fraude, signalez-le à votre service de police et au Centre antifraude du Canada, en ligne en utilisant le système de signalement en ligne ou en composant le 1-888-495-8501. Si vous n'êtes pas tombé dans le piège, signalez tout de même l'incident au CAFC.