BULLETIN DU CENTRE ANTIFRAUDE DU CANADA

Fraudes ciblant les entreprises 2024-10-22

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

En ce Mois de la sensibilisation à la cybersécurité, le CAFC tient à vous aider à protéger votre entreprise et à garder une longueur d'avance sur les fraudeurs. Qu'il s'agisse de faux comptes de médias sociaux, de courriels d'entreprises compromis, de détournement de paiement ou de rançongiciel, les menaces sont réelles et évoluent sans cesse. Il est plus important que jamais de faire preuve de vigilance et de protéger votre entreprise contre ces risques croissants.

Faux comptes de médias sociaux d'entreprises :
Les fraudeurs se servent de plus en plus de faux comptes ou de comptes clonés de médias sociaux d'entreprises pour envoyer des offres ou des messages frauduleux aux contacts, abonnés, clients et employés de ces entreprises. Par exemple, ils transmettront un message aux contacts et aux abonnées (inscrits dans le profil de l'entreprise légitime) les informant qu'ils ont gagné un cadeau publicitaire ou un concours et leur demandant de fournir leurs numéros de carte de crédit pour pouvoir toucher leur cadeau ou leur prix.

Conseils pour protéger votre entreprise

- Protégez vos comptes de médias sociaux. Assurez-vous de bien comprendre les conditions d'utilisation des plateformes de médias sociaux dont vous vous servez.
- Obtenez un compte « certifié » dans les médias sociaux. Les comptes « certifiés » offrent un niveau d'authenticité et de crédibilité.
- Surveillez régulièrement vos comptes de médias sociaux pour vous assurer qu'il n'y a pas de publications ou de messages inhabituels.
- Examinez l'information que vous diffusez. Peut-elle être utilisée pour créer de faux comptes ou faire parvenir des offres ou des demandes frauduleuses à vos clients et employés?
- Faites régulièrement des recherches dans les médias sociaux pour vérifier s'il existe de faux comptes de votre entreprise.
- Donnez des consignes claires ou des précisions sur les promotions, les concours ou l'envoi de cadeaux publicitaires.
- Faites parvenir des messages de sensibilisation à la fraude à vos clients et employés.
- Publiez des mises en garde si de faux comptes sont trouvés et signalez ceux-ci à la plateforme concernée.
- Obtenez d'autres conseils pour vous protéger.

Harponnage et détournement de paiement :
Pour ce type d'arnaque, 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 infiltrent ou mystifient le compte de courriel d'une entreprise ou d'un particulier, puis créer une règle pour qu'une copie des courriels entrants soit transmise à leur propre compte. Ils épluchent les courriels pour étudier le niveau de langue utilisé par l'expéditeur et cerner les habitudes liées à des contacts, à des dates et à des paiements importants.

L'attaque a lieu lorsque le titulaire du compte de courriel est difficilement joignable par courriel ou téléphone. Il pourrait s'agir d'un courriel semblant provenir d'un haut dirigeant d'une entreprise et destiné aux comptes créditeurs, dans lequel on demande un paiement urgent pour conclure un marché privé, ou d'un courriel semblant provenir d'un entrepreneur qui fournit de nouvelles modalités de paiement et demande le règlement d'une facture.

Conseils pour protéger votre entreprise

- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez vos employés.
- Offrez une formation sur la fraude aux nouveaux employés.
- Mettez en place des modalités de paiement détaillées, y compris une authentification verbale pour toute demande urgente ou tout changement dans les modalités de paiement.
- Exigez la vérification des demandes inhabituelles.
- Établissez des mesures d'identification, de gestion et de signalement des fraudes.
- N'ouvrez pas les courriels non sollicités et ne cliquez pas sur les pièces jointes ou les liens suspects.
- Passez le curseur de votre souris sur l'adresse de courriel ou le lien fourni pour en confirmer l'exactitude.
- Limitez la quantité d'information diffusée publiquement.
- Mettez à niveau et à jour vos logiciels de sécurité.
- Obtenez d'autres conseils pour vous protéger.

Rançongiciel :

La plupart des incidents de rançongiciel commencent par un courriel de harponnage ou d'hameçonnage renfermant une pièce jointe : un fichier exécutable, un document d'archives, une image ou un lien. Dès que la personne ouvre la pièce jointe ou clique sur le lien, le maliciel s'installe sur son système et peut demeurer inactif pendant plusieurs jours ou mois avant de chiffrer ou de verrouiller les fichiers ou les systèmes. Voici d'autres façons dont des réseaux ou des appareils peuvent être compromis :

• Vous consultez des sites Web non sécurisés, suspects ou compromis;
• Vous connectez un appareil externe infecté (p. ex. clé USB) à votre ordinateur;
• Vous exposez vos systèmes à Internet inutilement ou sans prendre de mesures robustes en matière de sécurité et de maintenance.

Conseils pour protéger votre entreprise

• Méfiez-vous des courriels non sollicités.
• Ne répondez pas aux courriels suspects et ne cliquez jamais sur les liens qu'ils renferment.
• Assurez-vous d'avoir un plan pour sauvegarder vos données systématiquement et fréquemment.
• Utilisez l'authentification à plusieurs facteurs et un anti-maliciel.
• Assurez-vous que des mises à jour et des correctifs sont apportés régulièrement à vos logiciels et systèmes, et que tous les mots de passe sont changés fréquemment.
• Publiez et mettez en application une politique sur la sécurité des employés.
• Collaborez avec les organismes d'application de la loi au moment d'élaborer et de mettre à l'essai un plan d'intervention en cas d'incident.
• Signalez tous les incidents!
• Consultez le site du CAFC pour obtenir d'autres conseils pour vous protéger.
• Consultez le site du Centre canadien pour la cybersécurité pour obtenir d'autres renseignements sur les rançongiciels et des conseils, des avis et des services en matière de cybersécurité.

Si vous croyez que votre entreprise a été la cible ou a été victime de cybercriminalité ou de fraude, vous devez le signaler à votre service de police local ainsi qu'au Centre antifraude du Canada au moyen de son système de signalement en ligne ou par téléphone au 1-888-495-8501. Il est important de signaler la fraude au CAFC même si vous n'êtes pas tombé dans le piège, car cela pourrait éviter que d'autres personnes en soient victimes.