Protection de votre entreprise – Guide de sensibilisation pour les employés

L'un des meilleurs moyens de se protéger des fraudes est de connaître les méthodes les plus couramment utilisées par les fraudeurs pour compromettre la sécurité des données et des systèmes.

Voici quelques renseignements qu'il est bon de garder à l'esprit concernant les fraudes dont votre entreprise pourrait être la cible.

Anatomie d'une fraude : Piratage psychologique

Bon nombre de fraudes visant les entreprises relèvent de la catégorie du «piratage psychologique», une méthode utilisée par les fraudeurs qui se fonde sur la manipulation et sur notre désir naturel d'aider et de répondre à des demandes urgentes.

Le piratage psychologique permet aux fraudeurs de contourner les protocoles de sécurité en profitant de nos faiblesses humaines.

Fraudes courantes visant les entreprises

L'hameçonnage est une forme de piratage psychologique qui consiste à utiliser des courriels mensongers pour amener les destinataires à divulguer de l'information personnelle ou financière pouvant être détournée à des fins malhonnêtes.

L'hameçonnage par téléphone, c'est l'équivalent de l'hameçonnage par courriel. Il consiste à utiliser le téléphone dans le but de soutirer des renseignements confidentiels pouvant ensuite être utilisés pour le vol d'identité ou pour réaliser un gain financier.

L'hameçonnage par message texte est une autre forme d'hameçonnage. Les fraudeurs envoient un message texte ou un SMS pour tenter d'obtenir des renseignements confidentiels ou pour pousser le destinataire à cliquer sur un hyperlien malveillant et à télécharger un maliciel sur son appareil.

Hameçonnage ciblé et fraude par compte de courriel d'entreprise compromis

Le harponnage est une forme plus ciblée d'hameçonnage, dont le but est d'inciter des personnes ou des petits groupes à transmettre des renseignements ou à installer un code malveillant sur leurs appareils. Cette technique s'appuie sur des technologies et des stratégies personnalisées plus développées pour contourner les filtres de courrier indésirable, et sur des tactiques de manipulation pour amener les destinataires à communiquer des renseignements confidentiels ou à accorder l'accès non autorisé à des comptes ou des systèmes.

La fraude par compte de courriel d'entreprise compromis vise les entreprises qui traitent régulièrement des paiements. Ce stratagème cible les employés qui ont accès à des données sensibles concernant l'entreprise ou les clients, et les responsables de la gestion des fournisseurs et des paiements. Les employés reçoivent par courriel des demandes de virements de fonds immédiats, de modification du numéro de compte ou de facture, ou d'accès à des données sensibles.

Les fraudeurs se font souvent passer pour un contact de confiance pour obtenir des données confidentielles, habituellement par courriel ou par un autre type de messagerie en ligne.

Les courriels falsifiés (ou courriels frauduleux) proviennent de fraudeurs qui se font passer pour des membres de la haute direction (chef de la direction, chef des Affaires financières) ou pour un collaborateur de confiance, et qui demandent un virement de fonds, un changement de compte ou l'accès à des données, des comptes ou des systèmes non autorisés.

Banque Scotia MD

Se protéger contre les différentes formes d'hameçonnage

- Souvenez-vous que ces fraudes contiennent souvent **des demandes urgentes ou provocantes** et que les expéditeurs se font passer pour des organisations légitimes ou pour des personnes que vous connaissez.
- **Vérifiez toujours l'adresse de l'expéditeur.** Méfiez-vous si celle-ci ne correspond pas à l'entreprise censée envoyer le courriel.
- **Prenez le temps de réfléchir.** Le sentiment d'urgence est-il vraiment justifié?
- Ralentissez et **évaluez attentivement les courriels**, les appels téléphoniques ou les textos qui contiennent une demande de renseignements confidentiels, de modification des détails du compte ou d'accès non autorisé.
- **Vérifiez l'identité** de la personne ou de l'organisation qui vous contacte en communiquant avec directement elle par téléphone, en utilisant un numéro de téléphone connu.
- **Méfiez-vous des pièces jointes ou des hyperliens** que vous ne vous attendiez pas à recevoir.
- Avant de cliquer sur un hyperlien, **placez votre curseur dessus** pour voir où il vous mènera. Si vous ne reconnaissez pas l'adresse qui s'affiche, ne cliquez pas dessus.

Logiciels malveillants

Par logiciel malveillant (maliciels), on entend tout logiciel conçu dans le but de voler des données sensibles, d'endommager ou de détruire des ordinateurs ou des systèmes informatiques.

Il existe une grande variété de maliciels : virus, vers, chevaux de Troie, logiciels-espions, logiciels publicitaires, rançongiciels. Ces derniers sont particulièrement utilisés aujourd'hui contre les entreprises. Ils peuvent attaquer et chiffrer (c'est-à-dire bloquer) les systèmes dans le but d'obtenir une rançon.

C'est généralement en téléchargeant un programme infecté qu'on installe involontairement un logiciel malveillant dans nos systèmes. Ceux-ci sont conçus pour avoir l'air légitimes; il arrive donc facilement qu'on les prenne pour un programme qu'on souhaiterait installer sur son ordinateur.

Les logiciels malveillants peuvent également être installés lorsqu'on ouvre ou télécharge une pièce jointe, ou qu'on sélectionne un hyperlien dans un courriel ou un message texte.

Se protéger contre les logiciels malveillants

- Assurez-vous d'avoir **un antivirus ou un antimaliciel** à jour sur vos appareils.
- Installez toujours **le système d'exploitation le plus récent** pour vos systèmes et vos appareils.
- Téléchargez des programmes uniquement de **sources sûres**, approuvées par votre entreprise.
- **Installez les correctifs et mettez à jour fréquemment les systèmes**, car les mises à jour contiennent généralement des correctifs de sécurité.
- **Faites preuve de vigilance quand vous naviguez sur Internet** et soyez à l'affût des indices qu'il s'agit d'un faux site Web (structure et mise en page de mauvaise qualité, absence de coordonnées de l'entreprise, fenêtres contextuelles, faux messages d'erreur).
- **Méfiez-vous toujours des pièces jointes et des hyperliens** provenant d'expéditeurs inconnus.

Fraude par télévirement

Les télévirements continuent à être la cible d'activités frauduleuses en raison de la vitesse et de la limite plus élevée des opérations. Les employés chargés de traiter les télévirements sont délibérément ciblés.

Parmi les méthodes courantes de fraude par télévirement, on retrouve les fraudes par compte de courriel d'entreprise compromis (piratage du courriel du client ou du fournisseur), prises de contrôle de compte, logiciels malveillants et hameçonnage (notamment par téléphone et par texto).

La fraude par télévirement survient souvent lorsqu'un fraudeur envoie un courriel se faisant passer pour un collaborateur de confiance et demande une modification des instructions de télévirement ou des détails du compte. Il peut demander une modification des renseignements relatifs au compte pour le paiement afin de recevoir les fonds sur un compte qu'il contrôle. Le courriel peut aussi contenir un hyperlien malveillant qui lance le téléchargement d'un maliciel sur votre appareil et votre réseau.

Se protéger contre la fraude par télévirement

- **Ne précipitez pas les choses** quand vous traitez des demandes de télévirement, même si elles sont urgentes.
- Prenez le temps de **vérifier la validité** des demandes de télévirement et de vous assurer que tous les protocoles sont respectés avant d'effectuer le virement.
- **Validez** toutes les demandes d'opérations inhabituelles en utilisant un numéro de téléphone sûr pour la personne en question.
- **Examinez régulièrement** les télévirements.
- **Tenez-vous au courant des habitudes** de vos clients et de vos fournisseurs, notamment quant à la fréquence et aux sommes habituelles de leurs opérations.
- **Informez** votre gestionnaire de toute demande de télévirement suspecte. Consignez toutes les communications et gardez une liste de personnes-ressources.

Informez votre gestionnaire de toute demande de télévirement suspecte. Consignez toutes les communications et gardez une liste de personnes-ressources.

Banque Scotia MD