Comment prévenir une tentative d'hameçonnage (pour les petites entreprises)

L'hameçonnage est l'une des escroqueries les plus courantes touchant la population canadienne à la maison et au travail. Les cybercriminels utilisent des messages d'hameçonnage pour tenter de voler des informations confidentielles aux gens en se faisant passer pour un expéditeur légitime, comme leur banque ou un collègue. Malheureusement, il est facile de tomber dans le piège de l'hameçonnage si vous ne savez pas quels signes repérer.

La cybersécurité est une responsabilité partagée, il est donc important que tous les membres de votre équipe sachent comment repérer les signes et combattre l'hameçonnage. Voici quelques mesures concrètes à prendre pour protéger votre entreprise :

Familiarisez-vous avec les signes de l'hameçonnage

Le meilleur moyen d'éviter les escroqueries par hameçonnage est de savoir en repérer les signes.

Un langage urgent ou menaçant

Faites attention aux messages vous incitant à répondre rapidement, surtout si la demande est étrange.

Des pièces jointes et des liens suspects

Méfiez-vous des liens dont l'URL n'est pas familière et des pièces jointes dont le nom ou le type de fichier (exe, par exemple) sont étranges et que vous n'avez pas demandées, surtout si l'expéditeur est suspect.

Des fautes de frappe

Faites attention aux adresses courriel incorrectes, aux liens suspects et à toute faute d'orthographe ou de grammaire inhabituelle.

Un graphisme non professionnel

Faites attention aux logos inexacts ou flous, ou aux courriels d'entreprise présentant des enjeux de formatage.

Des demandes d'informations confidentielles

Faites attention aux liens qui vous dirigent vers des pages de connexion et aux demandes concernant vos informations confidentielles (comme quelqu'un qui vous demande le mot de passe de votre compte).

Des messages inattendus

Faites attention aux factures que vous n'attendiez pas, ou aux demandes inattendues (comme votre patron qui vous demande des cartes-cadeaux dont vous n'avez pas discuté auparavant).

Sécurisez vos données et vos appareils

Les accidents se produisent. C'est pourquoi vous devez toujours avoir un plan de secours.

- Sécurisez votre réseau si vous travaillez à domicile ou si vous êtes en mode de travail hybride
- Faites des sauvegardes fréquentes de vos données et de vos appareils
- Demandez à votre employeur de vous parler du plan de cybersécurité de votre entreprise et familiarisez-vous avec ce plan
- Utilisez un réseau privé virtuel (RPV) si vous utilisez un réseau Wi-Fi non sécurisé
- N'utilisez pas vos appareils de travail à des fins personnelles et ne les prêtez pas à d'autres personnes
- Activez l'authentification multifactorielle lorsque possible

Apprendre à répondre à une escroquerie d'hameçonnage

Si vous êtes victime d'une tentative d'hameçonnage, ne paniquez pas.

- ✅ **Communiquez immédiatement avec votre service informatique** et informez-le de ce qui s'est produit. Si vous n'avez pas de service informatique dans votre entreprise, prévenez votre gestionnaire.
- ✅ Sécurisez votre compte **en changeant tout mot de passe compromis**.
- ✅ Assurez-vous que vos **nouveaux mots de passe sont robustes et uniques**.
- ✅ **Activez l'authentification multifactorielle** pour ajouter un niveau de sécurité supplémentaire à vos comptes et appareils.
- ✅ **Ne transférez pas le message à quelqu'un d'autre dans votre organisation.** Si vous avez besoin de partager le courriel, demandez à votre superviseur ou à un membre du service informatique de venir le voir sur votre écran.
- ✅ Déterminez qui est chargé (vous ou votre service informatique) de **signaler l'incident au Centre antifraude du Canada** en remplissant un signalement en ligne ou en l'appelant au **1-888-495-8501**.

Obtenez d'autres conseils pour protéger vos comptes et vos appareils :

PENSEZCYBERSECURITE.CA

1. CIRA, Sondage de CIRA sur la cybersécurité, Registre canadien de l'Internet, 2022

Catalogue number: D96-92/2022F-PDF | ISBN: 978-0-660-45575-4