SIX MOYENS SIMPLES DE

# Protéger votre entreprise des cybermenaces

**Alors qu'un grand nombre d'employés travaillent à distance et que les cybermenaces augmentent, les entreprises se doivent de connaître les mesures à prendre pour lutter contre la fraude. Partagez ce guide avec vos employés pour les aider à se protéger contre le cybercrime.**


## HAMEÇONNAGE PAR COURRIEL, TÉLÉPHONE OU TEXTO

**Des fraudeurs vous contactent par message texte ou par courriel en prétendant qu'ils représentent le gouvernement, une banque ou une entreprise.**

Ils vous dirigent vers un site qui n'a que l'apparence d'un site Web authentique. Puis, ils vous demandent de vérifier ou modifier votre mot de passe, vos comptes ou d'autres renseignements confidentiels.

## FRAUDES PAR COURRIEL

**Des criminels vous envoient un courriel en prétendant être un haut dirigeant de votre entreprise, un fournisseur de longue date ou une personne en qui vous avez confiance.**

Ils cherchent à vous convaincre de leur envoyer de l'argent par virement bancaire ou de leur fournir des renseignements confidentiels.

## LOGICIELS MALVEILLANTS

**Des criminels vous envoient un lien ou une pièce jointe par courriel, par message texte ou dans une fenêtre contextuelle.**

Lorsque vous cliquez sur un lien ou ouvrez une pièce jointe, des logiciels malveillants, aussi appelés maliciels, sont installés sur votre ordinateur. Les criminels utilisent un logiciel malveillant pour voler des renseignements et accéder à vos mots de passe, à vos questions de sécurité ou aux valeurs de vos jetons.

## 1 RÉFLÉCHISSEZ BIEN AVANT DE CLIQUER

**Méfiez-vous des liens inconnus suspects que vous recevez.**

Passez votre curseur sur les liens suspects pour vérifier où ils mènent. Soyez encore plus prudent si ces liens contiennent des caractères inhabituels, des traits d'union, des chiffres, des erreurs typographiques ou des symboles, ou s'ils vous dirigent vers des pages où l'on vous demande de fournir des renseignements confidentiels. Avant d'entrer un numéro de carte de crédit, vérifiez si l'URL commence par «HTTPS» et s'il s'agit d'un site sécurisé. Les sites «HTTP» ne sont pas sécurisés et les données entrées dans ces sites peuvent être compromises.

## 2 VÉRIFIEZ DEUX FOIS LES ADRESSES COURRIEL

**Vérifiez si l'adresse courriel de l'expéditeur est bien l'adresse courriel actuelle de votre fournisseur ou collègue.**

Déplacez votre curseur sur l'adresse de courriel pour l'afficher. Vous pouvez aussi glisser votre curseur sur n'importe quel lien pour afficher l'adresse URL en entier et vérifier où ce lien mène.

## 3 RESTEZ AU FAIT DES TENDANCES

**Renseignez-vous sur les tendances d'hameçonnage, de logiciels malveillants et de fraudes, afin de pouvoir les contrer.**

Demandez à vos employés de faire preuve de prudence en ce qui concerne les liens imprévus, les pièces jointes, les demandes inhabituelles de paiement ou les demandes de renseignements confidentiels. Consultez le Centre antifraude du Canada pour vous renseigner sur les derniers types de fraudes. N'oubliez pas que la Banque Scotia ne vous demandera jamais de fournir des renseignements confidentiels par courriel ou par texto.

## 4 SÉCURISEZ VOS MOTS DE PASSE

**Choisissez des mots de passe faciles à mémoriser, mais difficiles à deviner par d'autres personnes.**

Choisissez des mots de passe avec le plus grand nombre de caractères possible, qui combinent des chiffres, des lettres et des symboles. Mémorisez vos mots de passe plutôt que de les noter : une note écrite peut être lue, copiée ou volée.

## 5 PROTÉGEZ VOS APPAREILS À L'EXTÉRIEUR DU BUREAU

**Vous travaillez à l'extérieur? N'oubliez pas que les téléphones intelligents, les tablettes et les ordinateurs portables sont des objets faciles à voler.**

Surveillez constamment vos appareils et portez attention aux personnes présentes autour de vous. Aussi, évitez de travailler trop souvent dans des endroits publics offrant un service Wi-Fi, parce que ces réseaux sont moins sécurisés.

## 6 PLANIFIEZ LE DÉPART DES EMPLOYÉS

**Lorsqu'un employé quitte votre entreprise, vous devez rapidement lui retirer l'accès à vos locaux et à vos systèmes.**

Un compte non utilisé peut être repris rapidement par des pirates informatiques, et ce, sans que personne ne s'en rende compte.

## Vous aimeriez en savoir plus ?

**PROTÉGEZ-VOUS CONTRE LES ESCROQUERIES**
Obtenez plus d'information sur la fraude par courriel et par téléphone.

**PENSEZ CYBERSÉCURITÉ**
Découvrez comment améliorer la cybersécurité à la maison et au travail.

**CENTRE ANTIFRAUDE DU CANADA**
Restez au fait des derniers types de fraudes pour éviter d'en être victime.

**GUIDE DE CYBERSÉCURITÉ POUR PETITES ET MOYENNES ENTREPRISES**
Conseils pour la cybersécurité de votre entreprise.

Banque Scotia[MD]