7 CONSEILS DE SENSIBILISATION À LA CONFIDENTIALITÉ DES DONNÉES À L'INTENTION DES UTILISATEURS

1 Comprendre ce qui constitue une information personnelle

Une information personnelle réfère à tout élément de données qui, seul ou en combinaison, peut être utilisé pour identifier un individu. Il peut s'agir (entre autres) de votre adresse courriel, de votre numéro de téléphone, de votre numéro de passeport ou de permis de conduire, de vos documents médicaux ou financiers, d'adresses IP, de vos empreintes digitales et bien plus. Terranova Security recommande de partager ce type d'information seulement si nécessaire et uniquement avec des destinataires ou organisations de confiance, qui démontrent le respect de pratiques de confidentialité des données acceptables.

2 Utiliser des réseaux Wi-Fi sécurisés et un RPV

Pour minimiser les risques d'exposition des données, évitez de saisir des informations personnelles, y compris votre numéro de carte de crédit ou votre adresse, sur un réseau Wi-Fi public. Utilisez plutôt des points d'accès à Internet protégés par un mot de passe et, dans la mesure du possible, un réseau privé virtuel (RPV) pour plus de sécurité.

3 Vérifier la validité de l'URL du site Web

Avant de partager des informations personnelles en ligne, vérifiez la validité de l'adresse URL. Assurez-vous que le domaine contient « https:// » ou qu'un cadenas fermé apparaît à côté de la barre d'adresse dans votre navigateur. Même sur les sites sécurisés, Terranova Security recommande d'activer l'authentification à deux facteurs pour vos comptes en ligne, en particulier pour le commerce électronique.

4 Se méfier des tentatives d'hameçonnage

Les cybercriminels conçoivent des courriels d'hameçonnage dans le but de dérober les données personnelles des utilisateurs et de les utiliser pour commettre des vols d'identité ou mener d'autres activités malveillantes. Il est essentiel d'être vigilant en tout temps et de ne jamais partager des informations personnelles par courriel, à moins d'être certain de l'identité du destinataire et de la façon dont les données seront gérées et entreposées.

5 Connaître les autres types de cybermenaces

L'hameçonnage n'est pas la seule menace qui plane sur la confidentialité des données des utilisateurs. Soyez à l'affût des autres formes d'ingénierie sociale, comme l'hameçonnage par texto (messages textes) et par téléphone (messages vocaux). Ces communications frauduleuses, au ton urgent, semblent souvent provenir de sources connues et sont non sollicitées. En cas de doute, raccrochez et rappelez directement au numéro officiel.

6 Rapporter les demandes d'information suspectes

Les filtres antipourriel et autres précautions techniques n'assurent pas automatiquement le maintien de la confidentialité de vos données. Si vous remarquez des messages ou des activités suspectes qui peuvent avoir compromis vos informations personnelles, rapportez-les immédiatement à votre service des TI ou aux autorités compétentes.

7 Adopter la formation en sensibilisation à la sécurité

Les organisations et les individus qui traitent des données personnelles doivent respecter les meilleures pratiques de confidentialité. Pour assurer une protection complète de l'information, chacun devrait adopter au minimum un type de formation en sensibilisation à la sécurité et la compléter. Vous développerez ainsi les connaissances nécessaires pour protéger vos données, en plus de créer et de renforcer de bonnes habitudes en ligne.