LifeMatters®

Éviter les escroqueries

Les escroqueries se présentent sous toutes les formes et dans toutes les tailles. En voici quelques-unes que vous pouvez rencontrer :

- **Le hameçonnage (phishing) ou hameçonnage par SMS (smishing).** Vous recevez un courriel ou un SMS vous demandant de cliquer sur un lien. Le message prétend que vous devez agir rapidement sous peine de perdre l'accès à un compte ou à un service. Souvent, le lien vous dirige vers un faux site de paiement ou charge un logiciel malveillant sur votre appareil. De là, l'escroc peut voler vos renseignements personnels ou même prendre le contrôle de votre appareil.

- **Le harponnage (spear phishing).** Vous recevez un SMS ou un courriel d'une personne qui prétend être un ami ou un collègue. Elle vous demande d'envoyer de l'argent, de payer une facture ou de lui fournir vos renseignements personnels ou professionnels. Là encore, l'intention réelle est de voler de l'argent ou des renseignements ou d'accéder à un appareil ou au réseau d'une entreprise.

- **Le piratage psychologique (social engineering).** Les escrocs peuvent étudier vos médias sociaux pour faire du harponnage (spear phishing). Ils peuvent également utiliser ces renseignements pour vous proposer des escroqueries spécifiques, telles que des offres d'emploi de rêve, des opportunités de voyage, des consolidations de dettes ou des investissements. Gardez à l'esprit que si quelque chose semble trop beau pour être vrai, c'est probablement le cas.

Ces conseils vous aideront à reconnaître et à éviter les escroqueries :

- Si vous recevez un courriel suspect, vérifiez soigneusement l'adresse. Souvent, elle sera similaire (mais pas exactement identique) à l'adresse électronique officielle d'une organisation.

- Si une URL ne commence pas par « https:// », il peut s'agir d'un site Web dangereux ou frauduleux.

- Si la demande suspecte provient d'une personne que vous connaissez, vérifiez auprès d'elle par téléphone ou en personne avant d'agir. Si le message provient d'une entreprise avec laquelle vous faites affaire, appelez-la ou contactez-la par le biais de son site Web officiel.

- Si vous recevez un courriel ou un message frauduleux sur votre messagerie ou votre téléphone professionnel, suivez les procédures de l'entreprise pour signaler la tentative. Sur les appareils personnels, signalez et bloquez les courriels ou les numéros de téléphone frauduleux.

- Soyez prudent lorsque vous publiez des renseignements d'identification et d'autres détails personnels sur les sites de médias sociaux.

Si vous êtes victime d'une escroquerie, LifeMatters peut vous aider. Nous offrons une assistance 24 heures sur 24, 7 jours sur 7 et 365 jours par an pour gérer les conséquences juridiques et financières, y compris l'usurpation d'identité.

1-800-634-6433

Une assistance avec la vie, le travail, la famille et le bien-être
mylifematters.com • 24/7/365
Appelez en PCV le 262-574-2509 si vous êtes hors de l'Amérique du nord.
Des services ATS 711 et de traduction son disponibles.