Prévention du piratage psychologique: À faire et à ne pas faire

Prenez quelques minutes pour passer en revue notre liste de choses à faire et à ne pas faire si vous êtes aux prises avec une attaque de piratage psychologique.

On ne regrette jamais de prendre son temps, d'évaluer la communication que l'on vient de recevoir et de réfléchir avant de répondre, de cliquer sur des liens ou d'ouvrir des pièces jointes.

À faire

- Méfiez-vous de tout courriel, message texte ou appel téléphonique vous demandant de fournir des renseignements personnels ou financiers.
- Utilisez des mots de passe qui sont difficiles à deviner.
- Mémorisez vos mots de passe.
- Trouvez des phrases secrètes qui vous aideront à mémoriser vos mots de passe.
- Prenez le temps de vous renseigner au sujet d'une offre qui semble trop belle pour être vraie.
- Si une personne que vous connaissez vous demande, de manière inattendue, de partager vos renseignements personnels, communiquez avec elle par un autre moyen pour confirmer la demande.
- Placez le curseur de votre souris sur les adresses électroniques et les liens pour vérifier l'adresse de l'expéditeur ou la destination de l'URL.
- Soyez à l'affût des erreurs d'orthographe et de grammaire évidentes, ainsi que des logos, images et d'une mise en page de mauvaise qualité.
- Prenez garde aux appels douteux ou agressifs de personnes disant représenter la Banque Scotia.
    - ~ Si vous recevez ce type d'appel, raccrochez et signalez-le en nous appelant au **1-866-625-0561**

À ne pas faire

- N'ouvrez pas les pièces jointes et ne cliquez par sur les liens de courriels ou de messages textes provenant d'un expéditeur inconnu.
- N'appelez jamais le numéro de téléphone indiqué dans un courriel qui vous semble douteux.
- Ne partagez pas vos mots de passe ni vos NIP avec quiconque ni dans les applications ou les sites web qui vous demandent d'accéder à vos renseignements financiers, notamment les outils de gestion budgétaire comme Mint.
- N'utilisez jamais des appareils de stockage, comme un disque externe ou une clé USB, que vous trouvez dans un lieu public.
- Ne laissez jamais votre ordinateur, votre tablette ou votre appareil mobile sans supervision lorsque vous avez ouvert une session dans les services bancaires en ligne.
- Ne vous contentez pas de fermer votre navigateur lorsque vous avez terminé vos opérations bancaires en ligne; fermez la session en vous déconnectant.
- Ne cliquez jamais sur un lien dans un courriel ou une fenêtre intruse pour accéder à un site.
    - ~ Entrez plutôt vous-même l'adresse dans une nouvelle fenêtre de votre navigateur afin de vous assurer de vous brancher au site légitime de l'entreprise.

Banque Scotia MD