

Conseils de sécurité pour vous aider à rester en sécurité en ligne



Les conseils de sécurité suivants vous aideront à vous protéger, ainsi que votre argent, contre les cybercriminels :

Ignorez les appels, les messages texte ou les courriels non sollicités.

Si vous ne connaissez pas l'appelant ou l'expéditeur, évitez carrément de répondre au message ou à l'appel ou même de communiquer avec la personne. Si quelque chose vous semble douteux, raccrochez immédiatement et appelez l'entreprise en utilisant un numéro de téléphone de confiance, comme celui figurant sur son site Web légitime.

Protégez vos renseignements personnels.

Ne communiquez jamais vos numéros de compte, mots de passe, codes de vérification, NIP ou numéros d'assurance sociale à qui que ce soit.

Créez des mots de passe forts.

Choisissez un mot de passe différent pour chacun de vos comptes en ligne. Utilisez au moins huit caractères, en mélangeant lettres, chiffres et symboles. N'utilisez jamais de noms, d'anniversaires ou de suites courantes comme « 123456 ».

Sécurisez vos appareils.

Mettez régulièrement à jour vos appareils et vos applications, en particulier votre navigateur, ainsi que vos logiciels antivirus et pare-feu.

Réfléchissez avant de publier sur les médias sociaux.

En communiquant trop de renseignements en ligne et sur les médias sociaux, vous pouvez fournir des indices sur vos mots de passe ou sur vos questions de sécurité, facilitant ainsi l'accès des cybercriminels à vos comptes.

Reconnaissez les escroqueries courantes et les signes d'alerte.

Évitez de cliquer sur les pièces jointes de sources inconnues ou suspectes. Ne fournissez pas (ou ne mettez pas à jour) des renseignements personnels au moyen de liens ou d'URL reçus par appel téléphonique, par message texte ou par courriel.

Prenez votre temps et évitez de répondre à des demandes « urgentes ».

Ne vous précipitez pas pour répondre ou réagir face à des demandes urgentes ou à des offres qui semblent trop belles pour être vraies.

Inscrivez-vous aux alertes des services bancaires.

L'une des façons de contribuer à protéger vos comptes est de vous inscrire aux alertes de votre banque, comme les Alertes BMO. Elles vous permettent de faire facilement le suivi des transactions portées à votre compte et de repérer toute transaction douteuse.

Examinez attentivement les adresses courriel et les URL.

Les courriels et les sites Web peuvent sembler être le fait d'entreprises de confiance, mais si vous examinez attentivement l'adresse courriel et URL, vous remarquerez de petites différences, comme une lettre supplémentaire, un point ou un nom de domaine différent (p. ex. « .net » au lieu de « .com »).

Utilisez l'authentification multifactorielle.

L'authentification multifactorielle peut contribuer à prévenir l'usurpation d'identité et la prise de contrôle de comptes, car elle utilise plus d'une méthode (comme un code d'accès unique) pour confirmer qu'il s'agit bien de vous.

Rappel

BMO ne communiquera jamais avec vous par courriel, par message texte ou par téléphone sans être sollicité afin de vous demander votre numéro de carte bancaire ou votre NIP, des renseignements confidentiels, des mots de passe ou des codes de vérification (codes d'accès à usage unique). BMO ne communiquera jamais avec vous pour vous demander votre numéro de carte bancaire ou votre NIP, ni n'enverra un messenger chercher votre carte ou votre NIP.

Si vous recevez un appel, un message vocal, un courriel ou un message texte d'une personne prétendant provenir de BMO et que vous trouvez cela suspect, ne fournissez aucun renseignement personnel et communiquez immédiatement avec nous en utilisant les renseignements figurant au verso de votre carte.

À BMO, votre sécurité est notre priorité. Pour en savoir plus sur la prévention de la fraude, visitez le site [BMO.com/securite](https://www.bmo.com/securite).