Sécurité client et communication sur le site Web sur la sensibilisation à la fraude

Notre approche de la sécurité

Quand il s'agit de vos informations financières, votre sécurité est notre priorité absolue. Lors de votre accès à votre compte électronique e-money, nous devons vérifier votre identité. Voici comment nous procédons.

Détails de connexion

Nous vous fournissons des informations de connexion en ligne uniques pour vous, pour vous protéger, nous vous recommandons de ne pas les partager.

Questions peersonnelles

Si vous contactez notre service clientèle, nous pouvons vous demander de confirmer votre identité en vous demandant de fournir les réponses aux questions personnelles que vous avez fournies lors de la création de votre compte électronique e-money en ligne.

Un code unique

Nous envoyons ces codes uniques à usage unique à votre adresse e-mail, fournie par l'administrateur de votre entreprise, pour plus de sécurité quand :

- périodiquement lors de la connexion juste pour confirmer votre identité ;
- lorsque vous demandez à modifier vos informations personnelles.

Fournir des informations

Nous ne vous demanderons jamais vos détails de mot de passe en ligne ni votre code PIN. Nous vous demanderons toujours d'utiliser notre application Milo ou notre site web libre-service.

Comment signaler une fraude

Si vous remarquez quelque chose de suspect et soupçonnez une fraude, vous devez nous contacter dès que vous en avez connaissance en utilisant le [numéro de téléphone] [adresse e-mail][dans la notification application].

Signaler une fraude :	servicedesk@xximo.be ou 078 – 353 452
Cartes perdues ou volées :	078 – 353 452
E-mails suspects :	servicedesk@xximo.be ou 078 – 353 452

Comment se protéger de la fraude

Aidez-vous à vous protéger des fraudeurs en suivant les conseils ci-dessous. Merci de noter que si vous avez un doute, veuillez ne pas prendre d'action. Une véritable entreprise ne vous poussera jamais à agir.

Assurez-vous toujours que votre numéro de téléphone portable et votre adresse e-mail enregistrés auprès de nos services sont à jour, nous les utiliserons pour vous contacter si nous remarquons une activité inhabituelle sur votre compte électronique e-money.

Quelques conseils pour utiliser votre compte électronique e-money et carte prépayée en toute sécurité

Lorsque vous accédez à votre compte électronique e-money en ligne :

- Utilisez un logiciel antivirus et un pare-feu.
- Veuillez à garder votre ordinateur et votre navigateur à jour.
- Utilisez des réseaux sécurisés.

- Utilisez des mots de passe forts.
- Ne partagez aucun mot de passe, y compris les mots de passe à usage unique qui vous ont été envoyés.

Lors de l'utilisation d'une application mobile :
- Installez uniquement les applications des magasins d'applications reconnus.
- Considérez les évaluations et les commentaires de l'application.
- Soyez conscient des autorisations que vous accordez.
- Traitez votre téléphone comme votre portefeuille.

Lorsque vous faites des achats en ligne ou dans un magasin :
- Lorsque vous utilisez une boutique en ligne pour la première fois, faites des recherches pour vous assurer que cette boutique existe bien.
- Ne répondez pas aux courriels non sollicités de sociétés que vous ne reconnaissez pas.
- Avant de saisir les détails de votre carte prépayée, assurez-vous que le lien est sécurisé. Il devrait y avoir un symbole de cadenas dans la fenêtre du navigateur qui apparaît lorsque vous vous connectez ou vous enregistrez. Si ce symbole apparaît sur la page plutôt que sur le navigateur, cela peut indiquer un site web frauduleux. L'adresse Web devrait commencer par https://, le «s» signifie sécurisé.
- Veuillez toujours vous déconnecter du site après utilisation. La simple fermeture de votre navigateur ne suffit pas pour garantir la sécurité de vos données.
- Gardez votre code PIN en sécurité et ne le partagez pas.
- Saisissez votre code PIN à l'abri des regards indiscrets et cachez votre code PIN.
- Vérifiez toujours vos relevés.

N'oubliez pas que si vous décidez de donner, de revendre ou de recycler un ancien téléphone portable, ordinateur, ordinateur portable ou tablette, assurez-vous de supprimer d'abord toutes les données et applications. Sinon, elles peuvent être consultées par tous les utilisateurs..