Bericht klantveiligheid en fraude-awareness website

Onze aanpak i.v.m. veiligheid

Wanneer het aankomt op uw financiële informatie, is uw veiligheid een topprioriteit voor ons en als u uw e-money account opent, is het belangrijk voor ons te weten dat u het bent. Dit zijn enkele manieren waarop wij dit doen.

Login details
Wij bezorgen u online login gegevens die uitsluitend voor u werden gepersonaliseerd. Om uzelf te beschermen, raden wij u aan deze niet met anderen te delen.

Herinneringsvragen
Als u contact opneemt met onze servicedesk, is het mogelijk dat wij u vragen wie u bent door u de antwoorden op de herinneringsvragen te laten geven toen u uw online e-money account creëerde.

Eenmalige toegangscode
Wij sturen deze unieke eenmalige codes naar uw e-mailadres, verstrekt door de administrator van uw bedrijf, voor extra veiligheid:

- periodiek bij login, gewoon om te weten of u het wel degelijk bent;
- als u vraagt veranderingen aan te brengen in uw persoonlijke gegevens.

Geven van informatie
Wij zullen u nooit om uw online password gegevens of uw PIN nummer vragen. Wij zullen u altijd vragen om onze Milo app of selfservice website te gebruiken.

Hoe kunt u fraude rapporteren?

Mocht u iets verdachts opmerken en vermoeden dat het om fraude gaat, dan vragen wij u zo snel mogelijk contact met ons op te nemen via onderstaande gegevens.

Fraude rapporteren:	servicedesk@xximo.be of 078- 353452
Verloren of gestolen kaarten:	078- 353452
Verdachte e-mails:	servicedesk@xximo.be of 078- 353452

Hoe kunt u uzelf beschermen tegen fraude?

Help uzelf te beschermen tegen fraudeurs door onderstaande tips op te volgen. Onthoud dat u niet handelt bij twijfel. Een betrouwbare firma zal u nooit dwingen meteen te beslissen.

Zorg er altijd voor dat het gsm-nummer en het e-mailadres dat bij ons is geregistreerd, up-to-date is. Wij zullen deze gebruiken om u te contacteren als we ongewone activiteit opmerken op uw e-money account.

Enkele tips voor veilig gebruik van uw e-money account en prepaid card

Bij het online aanloggen in uw e-money account

- Gebruik antivirussoftware en firewall.
- Houd uw computer en browser up-to-date.
- Gebruik veilige netwerken.
- Gebruik sterke wachtwoorden.
- Deel geen enkel wachtwoord, ook niet de eenmalige wachtwoorden die u worden toegestuurd.

Bij het gebruik van een mobiele applicatie

- Installeer enkel apps van erkende app-stores.
- Houd rekening met de app-ratings en reviews.
- Let op welke toelatingen u geeft.
- Bescherm uw telefoon net zoals uw portefeuille.

Bij online aankopen of in een winkel

- Als u een online winkel voor het eerst gebruikt, doe dan eerst een beetje research om te weten of die betrouwbaar is.
- Antwoord niet op ongevraagde e-mails van firma's die u niet herkent.
- Vóór u uw prepaid card gegevens invult, checkt u of de verbinding veilig is. In de rand van de zoekbalk moet een hangslotsymbool verschijnen als u inlogt of registreert. Als het in de pagina zelf verschijnt in plaats van in de zoekbalk, kan dit wijzen op een frauduleuze website. Het webadres moet beginnen met https://, de 's' betekent secure = veilig.
- Log na gebruik altijd uit op de website. Gewoon de browser sluiten is niet voldoende om u ervan te verzekeren dat uw data veilig is.
- Bewaar uw PIN-nummer op een veilige plaats en deel het niet.
- Als u uw PIN-nummer ingeeft, let dan op of er geen mensen rondom u staan en verberg uw PIN-nummer.
- Kijk altijd uw rekeninguittreksels na.

Onthoud dat als u beslist een oude gsm, computer, laptop of tablet weg te schenken, te verkopen of te recycleren, u al uw data en apps volledig moet verwijderen omdat deze anders overgaan naar diegene die uw toestel in handen krijgt.