Bericht over klantveiligheid en fraude-awareness website

Onze aanpak van beveiliging

Als het over uw financiële informatie gaat, is uw veiligheid een topprioriteit voor ons en als u uw e-money account opent, is het belangrijk voor ons om vast te stellen dat u het bent. Dit zijn enkele van de manieren waarop wij dit doen.

Logingegevens

Wij verstrekken u unieke online logingegevens. Om uzelf te beschermen, raden wij u aan deze niet met anderen te delen.

Herinneringsvragen

Als u contact opneemt met onze servicedesk, kan het gebeuren dat wij u vragen om uw identiteit te bevestigen door de antwoorden op de herinneringsvragen te geven die u heeft doorgegeven bij het opzetten van uw online e-money account.

Eenmalige toegangscode

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

- periodiek bij het inloggen, gewoon om te controleren dat u daadwerkelijk de persoon bent die inlogt;
- als u ons vraagt om veranderingen aan te brengen in uw persoonlijke gegevens.

Verstrekken van informatie

Wij zullen u nooit vragen om uw online wachtwoordgegevens of pincode. Wij zullen u altijd vragen om onze Milo app of selfservice website te gebruiken.

Hoe u fraude kunt melden

Als u iets verdachts opmerkt en vermoedt dat het om fraude gaat, neem dan zo spoedig mogelijk contact met ons op via [telefoonnummer] [e-mailadres][appmelding].

Fraude melden:	servicedesk@xximo.nl of 0900 - 1980
Verloren of gestolen kaarten:	0900 - 1980
Verdachte e-mails:	servicedesk@xximo.nl of 0900 - 1980

Hoe u zich kunt beschermen tegen fraude

U kunt zich beschermen tegen fraudeurs door de onderstaande tips op te volgen. Onthoud dat u nooit moet handelen als u ergens twijfels over heeft. Een bonafide bedrijf zal u nooit opjagen om meteen actie te ondernemen.

Zorg dat het mobiele nummer en het e-mailadres die bij ons geregistreerd staan up-to-date zijn. Wij gebruiken deze contactgegevens om u te contacteren als wij ongewone activiteiten opmerken op uw e-money account.

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

Bij online inloggen in uw e-money account

- Gebruik een antivirussoftware en firewall.
- Houd uw computer en browser up-to-date.
- Gebruik beveiligde netwerken.
- Gebruik sterke paswoorden.
- Deel geen enkel wachtwoord, ook niet de eenmalige wachtwoorden die wij u toesturen.

Als u een app op uw mobiel gebruikt

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

Als u online of in een webwinkel een aankoop doet

- Als u voor het eerst een webwinkel gebruikt, doe dan eerst wat research om te bepalen of die vertrouwd is.
- Reageer niet op ongevraagde e-mails van bedrijven die u niet kent.
- Controleer of de verbinding veilig is voordat u de gegevens van uw prepaid card invult. In de rand van de zoekbalk moet een hangslot symbool verschijnen als u inlogt of zich 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 altijd uit op de website uit na gebruik. Gewoon de browser sluiten is niet voldoende om te garanderen dat uw gegevens veilig zijn.
- Bewaar uw pincode op een veilige plaats en deel deze niet met anderen.
- Als u uw pincode invoert, let dan op dat er geen mensen in de buurt staan en zorg dat uw pincode niet kan worden afgekeken.
- Controleer altijd uw bankafschriften.

Onthoud dat als u een oude mobiele telefoon, computer, laptop of tablet doneert, verkoopt of recyclet, u altijd al uw gegevens en apps volledig moet verwijderen omdat deze anders in handen van de volgende gebruiker kunnen komen.