

Belangrijke boodschap!

Wapen u tegen verhoogde phishing activiteit

Beste klant,

Wij stellen de laatste weken een verhoogd risico op phishing vast.

Phishing gebeurde totnogtoe via e-mail, telefoon of sms, maar de criminelen worden steeds creatiever. Wist u dat ze ook uw vertrouwelijke bankgegevens proberen te ontfutselen via valse loginpagina's die lijken op die van uw bank?

Wij willen u helpen om u zo goed mogelijk te wapenen tegen deze vorm van fraude.

Lees daarom aandachtig ons advies op de volgende pagina's.

Voor vragen omtrent phishing kan u steeds terecht bij:

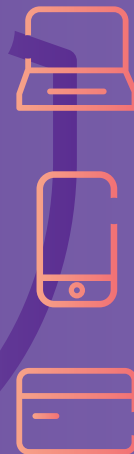
- Uw **Beobank kantoor**
- Ons **Beobank Service Center** op **02 622 20 00**

Een verdachte e-mail kan u doorsturen naar **phishing@beobank.be**

Om een fraudegeval te melden, vul het contactformulier op onze website in.

Veilige groeten,
Beobank

5 tips om u te wapenen tegen PHISHING



1



Geef nooit uw geheime gegevens :

- **wachtwoord,**
- **kredietkaartnummer,**
- **codes** voor internetbankieren,
- **enz.**

door via **telefoon**, via **een link** in een e-mail of een sms, op **sociale netwerken** of **websites** die u niet kent.

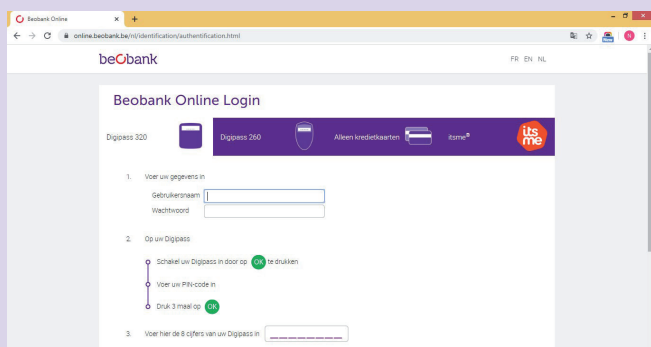
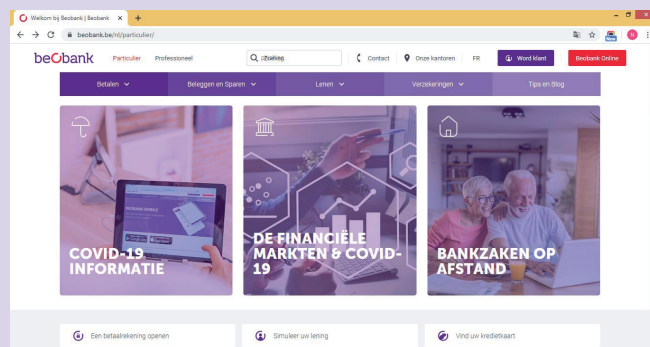
2

Dit zijn de **officiële Beobank adressen:**

De Beobank website:

<https://www.beobank.be>

Hier vindt u alle informatie over Beobank en haar diensten en producten terug.



Beobank Online:

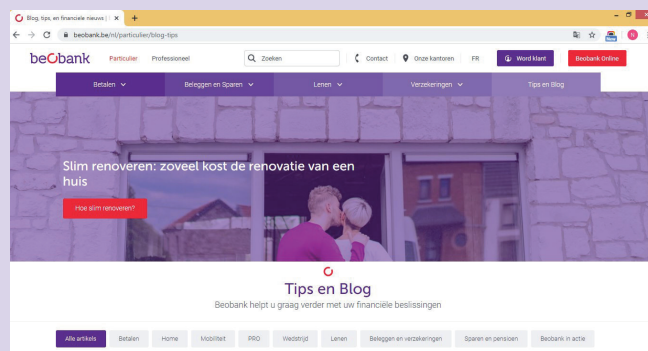
<https://online.beobank.be/nl>

Voor internetbankieren.

De Beobank blog:

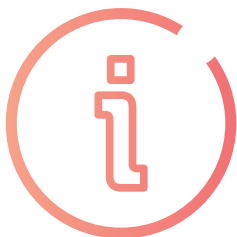
<https://www.beobank.be/nl/particulier/blog-tips>

Hier vindt u interessante artikels terug rond de actualiteit.



3

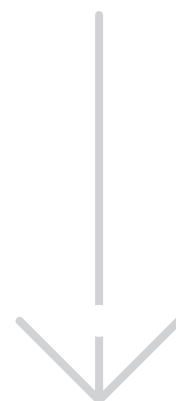
Herken op tijd verdachte berichten



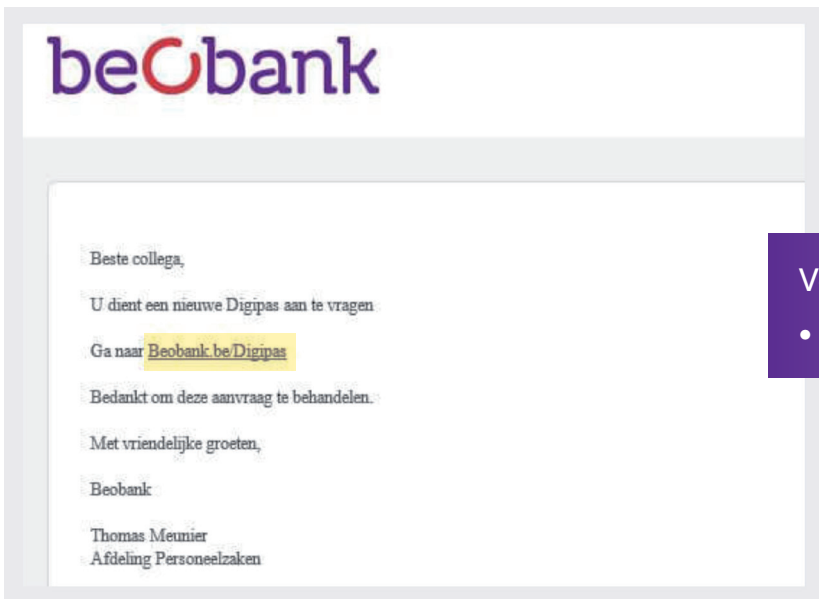
Verdachte berichten zijn vaak te herkennen aan enkele kenmerken.

- Phishingberichten komen **meestal onverwacht en zonder reden**.
- De taal is **dwingend of wil u nieuwsgierig** maken.
- Ze bevatten soms **taalfouten** of zijn **niet professioneel** opgemaakt.
- Een **vage aansprektitel** of uw e-mailadres als aanspreking kan verdacht zijn.
- **Onbekende afzenders** of **foute e-mailadressen** moeten uw aandacht trekken.
- Bevat het bericht een link? Klik niet zomaar! **Wees steeds op uw hoede als u een link ontvangt in een e-mail of SMS die naar een inlogpagina verwijst.**
- Berichten die **in uw Spam/Junk folder** terecht komen, moet u zeker wantrouwen.

(zie voorbeelden van verdachte berichten op de volgende pagina)



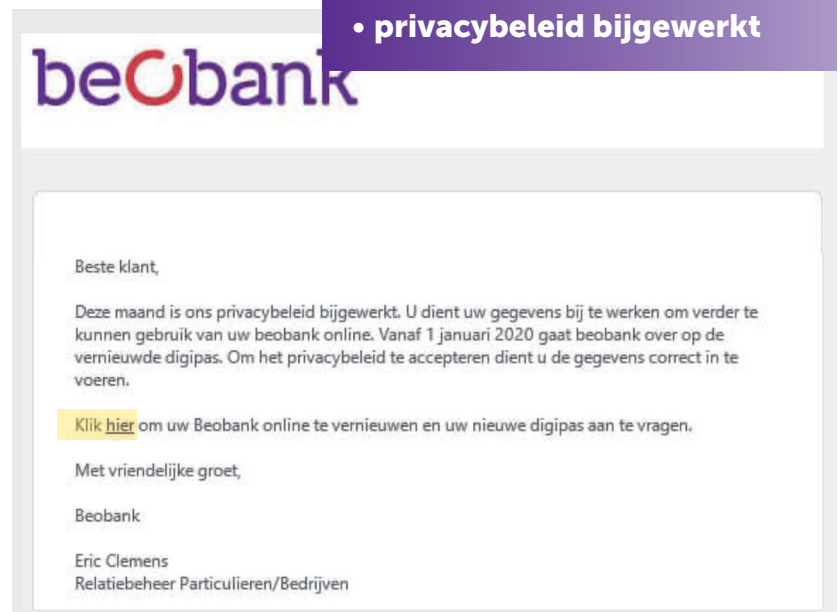
Voorbeelden van verdachte berichten



Voorbeeld frauduleuze e-mail:
• nieuwe **digipas**



Voorbeeld frauduleuze SMS:
• **Card Stop**



Voorbeeld frauduleuze e-mail:
• **privacybeleid bijgewerkt**



Voorbeeld frauduleuze e-mail:
• **domiciliëring**



4

Praktische tips

Volg deze tips om fraudeurs te slim af te zijn en veilig te bankieren.

- **Geef uw wachtwoorden en geheime codes nooit door aan de telefoon**, ook al werkt degene die u belt zogezegd voor een bedrijf dat u kent of waar u klant bent.
- **Controleer altijd of e-mails van het officiële e-mailadres komen** (vb. @beobank.be) en klik nooit op een link naar een website waar men u vraagt uw bankgegevens en -codes in te geven.
- **Geef enkel uw toegang- en bankcodes in** op onze <https://www.beobank.be> website of in de officiële Beobank-app.
- **Laat uw uittreksels of bankdocumenten** (met bankgegevens) niet rondslingeren.
- Hebt u een Beobank kredietkaart? **Schrijf u dan in op de dienst Beobank Alert**. Dan krijgt u van ons een sms of e-mail als uw kredietkaart wordt gebruikt voor een transactie van 150 € of meer.
- Als u een betaling uitvoert, **controleer dan nogmaals het bedrag** vooraleer u de betaling bevestigt.
- **Installeer een antivirusprogramma** op uw computer en voer regelmatig updates uit.
- **Terugbetalingen moeten nooit bevestigd worden** met een code gegenereerd door uw digipass of via een sms code.
- Bij twijfel kunt u ons altijd om raad vragen. Bel uw Beobank agentschap of stuur een e-mail naar phishing@beobank.be
Om een fraudegeval te melden, vul het contactformulier op onze website in.

5

Belangrijk!

Hebt u een frauduleuze e-mail of SMS ontvangen: informeer ons dan onmiddellijk via phishing@beobank.be

Om een fraudegeval te melden, vul het contactformulier op onze website in.

Hebt u per ongeluk toch uw kaartgegevens doorgegeven?

Neem dan direct contact op met **Card Stop** op **078 170 170** of met uw bank, zodat uw rekeningen, kaarten en toegangscodes kunnen geblokkeerd en veranderd worden

Meer nuttige tips en voorbeelden van phishing e-mails vindt u op onze website of op <https://www.safeonweb.be>