



Message important !

Armez-vous contre l'augmentation des tentatives de phishing

Chère cliente, Cher client,

Nous avons identifié un risque accru de phishing au cours des dernières semaines.

Jusqu'à présent, le phishing, s'effectuait principalement par e-mail, par téléphone ou par SMS, mais les criminels deviennent de plus en plus créatifs et inventifs.

Effectivement, depuis quelque temps, ils essaient aussi d'obtenir vos données bancaires via des fausses pages de connexion ressemblant à celles de votre banque.

Nous voulons vous aider à vous protéger au mieux contre cette forme de fraude.

Veuillez lire attentivement nos différents conseils repris dans les pages suivantes.

Pour des questions sur le phishing, vous pouvez toujours contacter :

- Votre **agence Beobank**
- Notre **Beobank Service Center** au **02 622 20 00**

Vous pouvez envoyer un e-mail suspect à **phishing@beobank.be**

Pour signaler une fraude, veuillez remplir le formulaire de contact disponible sur notre site Internet (www.beobank.be/fr/particulier/phishing).

Salutations,
Beobank

5 conseils pour vous armer contre le PHISHING



1



Ne fournissez jamais vos données secrètes telles que :

- votre **mot de passe**,
- votre **numéro** de carte de crédit, la **date d'expiration** et le **code CVV** (au recto)
- vos **codes** pour les services bancaires par Internet,
- **etc.**

Par **téléphone**, via **un lien** dans un e-mail ou un SMS, sur les **réseaux sociaux** ou sur des **sites Internet** que vous ne connaissez pas.

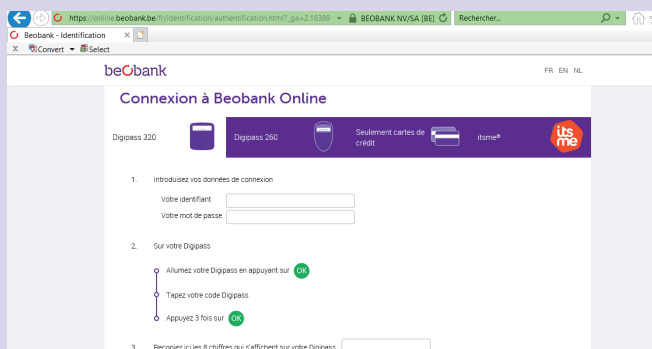
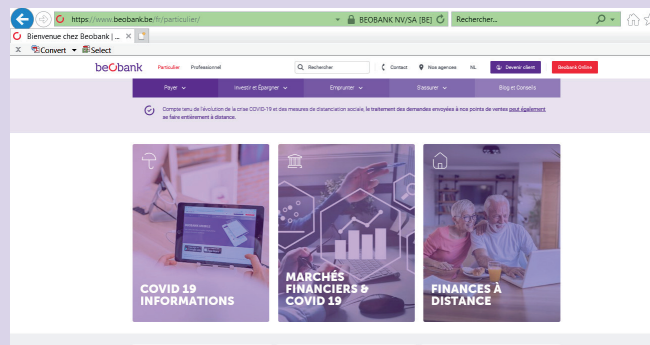
2

Voici les **adresses officielles de Beobank** :

Le site web de Beobank :

<https://www.beobank.be>

Vous trouverez ici toutes les informations sur Beobank, ses services et ses produits.



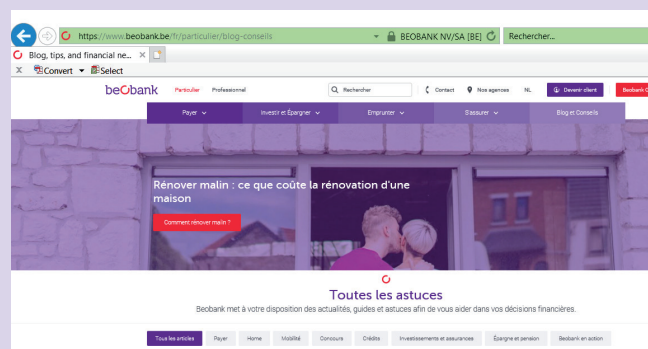
Beobank Online:

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

Pour vos opérations bancaires par Internet.

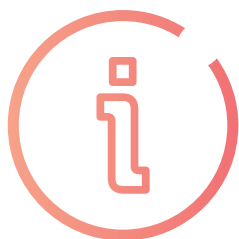
Le blog officiel de Beobank :
<https://www.beobank.be/fr/particulier/blog-conseils>

Vous y trouverez des articles intéressants traitant de l'actualité.



3

Reconnaître à temps les messages suspects



Les messages suspects se reconnaissent généralement à quelques caractéristiques :

- Les messages de phishing **arrivent souvent inopinément et sans raison.**
- Le langage utilisé est **contraignant** ou **conçu pour éveiller votre curiosité.**
- Ils contiennent souvent des **fautes d'orthographe et/ou de grammaire** et ne sont **pas rédigés de manière professionnelle.**
- Un **titre vague** ou votre adresse e-mail en guise de titre peuvent être suspects.
- Des **expéditeurs inconnus** ou des **adresses e-mail erronées** doivent attirer votre attention.
- Le message comporte un lien ? Ne cliquez jamais dessus directement ! **Méfiez-vous toujours si vous recevez un lien dans un e-mail ou un SMS qui vous dirige vers une page de connexion.**
- Méfiez-vous des messages qui atterrissent **dans votre boîte Spam/Junk.**

(Voir des exemples de messages suspects à la page suivante)



Exemples d'e-mails frauduleux

Nouvelle année, nouveau Digipass! Demandez gratuitement te nouveau Digipass

Cher Monsieur/Madame,

Beobank lance son nouveau Digipass amélioré. Le nouveau Digipass offrira une meilleure protection contre les activités frauduleuses. Beobank met tout en œuvre pour garantir à ses clients un environnement en ligne sécurisé.

Notre clientèle a montré que vous utilisiez toujours le Digipass obsolète malgré plusieurs rappels. Vous avez la possibilité de demander le Digipass jusqu'au 10 janvier 2019, après cette date, nous sommes obligés de mettre temporairement votre compte en attente.

Nous vous demandons par la présente de vous inscrire via le bouton ci-dessous.

[S'inscrire](#)

[cliquez ici si les images ne sont pas automatiquement visibles sur votre appareil.](#)

Nous sommes convaincus que vous nous avez suffisamment informés.

• nouveau digipass

• mise à jour de la politique de confidentialité

Van: Beobank [mailto:cettina@montatorparquet.ro]
Verzonden: donderdag 17 januari 2019 7:29
Onderwerp: Dringende aandacht/Attention urgente

beObank

Cher client,

Nous n'avons pas pu vous joindre par téléphone, ce qui vous a envoyé cet e-mail comme alternative. Lors de notre récente vérification de sécurité des comptes de tous nos clients, nous avons constaté des problèmes de sécurité sur votre compte bancaire en ligne. Veuillez prendre un moment pour vérifier votre compte afin d'éliminer la menace et garder votre compte à l'abri de toute activité frauduleuse.

Vérifier le compte via l'URL ci-dessous.

<https://www.beobank.be/fr/verify>

L'absence de vérification du compte exposera votre compte à des risques et vous ne pourrez pas accéder à votre compte bancaire en ligne pour des raisons de sécurité, ce qui nécessitera votre présence physique dans votre agence bancaire avant de pouvoir accéder à votre compte. Désolé pour l'inconvénience.

Cordialement
Banque Allemande.

• nouvelle mise à jour de sécurité

Vers: Beobank Alert <customer.service@beobank.be>
Verzonden: uursdag 22 mei 2019 9:14
Aan: undisclosed-recipients:....
Onderwerp: Notification/Kenngeving

beObank

Cher client,

Beobank nouvelle mise à jour de sécurité.

Nous mettons à jour nos services afin de fournir une meilleure expérience pour le nouveau serveur SSL, qui commence le 21 mai 2019. Mettez à jour votre profil avec le lien ci-dessous.

Digipass1 <https://www.online.beobank.be/ecct/verify/KVA2B71>

Digipass2 <https://www.online.beobank.be/scct/verify/GVA7B53>

Meilleures salutations,
Département de sécurité de Beobank.

• „Nous introduisons la nouvelle carte de paiement à puce NFC”

beObank

Nous introduisons

la nouvelle carte de paiement à puce NFC

Cher client,

En tant que client, vous souhaitez être informé clairement et à nos produits et services. Puisque vous avez un compte de paiement chez nous, nous sommes heureux de vous informer de nos nouveaux développements.

Introduction Beobank Online

Beobank présente avec Beobank Online une nouvelle carte de paiement avec puce NFC et un digipass avec un nouveau logiciel de sécurité. Cela permet de se connecter d'une nouvelle manière. Avec la nouvelle carte de débit et le digipass de Beobank Online, vous pouvez vous connecter à votre Beobank-Online en tenant votre carte débit contre votre digipass et en la numérisant. Vous pouvez désormais payer sans contact en gardant votre carte de débit à proximité d'un terminal de paiement situé dans le magasin, à condition qu'elle soit équipée d'un terminal NFC.

Pour des raisons de sécurité, il est conseillé de demander dès que possible la carte de paiement renouvelée et le digipass. Beobank Online vous protège mieux contre la fraude par carte de débit. L'émission de la carte de paiement et des digipass Beobank Online est gratuite jusqu'au 14 janvier 2019. Ensuite, un montant de 39,95€ sera facturé.

Inscrivez-vous maintenant pour la carte de débit et le digipass Beobank Online avec un nouveau design!

[S'inscrire](#)

Nous sommes convaincus que vous nous avez suffisamment informés.



4

Conseils pratiques

Suivez ces conseils pour déjouer les fraudeurs et effectuer vos opérations bancaires en toute sécurité.

- **Ne communiquez jamais votre mot de passe et vos codes bancaires secrets par téléphone**, même si la personne qui vous appelle travaille soi-disant pour une société que vous connaissez ou dont vous êtes client.
- **Vérifiez toujours si les e-mails proviennent de l'adresse e-mail officielle** (par exemple @ **beobank.be**) et cliquez jamais sur un lien vers un site Web où vous êtes invité à entrer vos coordonnées bancaires et vos codes.
- **Ne donnez vos codes d'accès et bancaires que sur notre site web Beobank** (dont l'adresse débute par **https://www.beobank.be/**) ou dans l'application officielle **Beobank Mobile**.
- **Ne laissez pas traîner vos relevés ou documents bancaires** (avec les coordonnées bancaires).
- Vous avez une carte de crédit Beobank ? **Alors inscrivez-vous au service Beobank Alert**. Nous vous enverrons alors un sms ou un e-mail lorsque votre carte de crédit est utilisée pour une transaction de 150 euros ou plus.
- Lorsque vous effectuez un paiement, **vérifiez une dernière fois le montant** avant de confirmer la transaction.
- **Installez un programme antivirus** sur votre ordinateur et mettez-le régulièrement à jour.
- **Les remboursements ne doivent jamais être confirmés** avec un code généré par votre digipass ou via un code SMS.
- En cas de doute, vous pouvez toujours nous demander de l'aide. Appelez votre agence Beobank ou envoyez un mail à **phishing@beobank.be**. Pour signaler une fraude, veuillez remplir le formulaire de contact sur notre site Internet.

5

Important !

Si vous avez reçu un e-mail ou un SMS frauduleux : veuillez-nous en informer immédiatement via **phishing@beobank.be**

Pour signaler une fraude, veuillez remplir le formulaire de contact sur notre site internet.

Avez-vous accidentellement transmis les informations de votre carte ?

Veuillez contacter Card Stop directement au **078 170 170** ou votre banque, afin que vos comptes, vos cartes, vos codes d'accès puissent être bloqués et modifiés.

Plus de conseils utiles et exemples d'e-mails de phishing sont disponibles sur notre site web et via **https://www.safeonweb.be**