Apprenez à vous protéger contre la fraude

do your thing

En tant que banque en ligne, ING vous propose toujours plus d'outils numériques pour vos activités bancaires. Les transactions bancaires en ligne sont faciles et vous offrent plus de liberté et plus de temps. Mais peut-être ne vous sentez vous pas encore en sécurité lorsque vous utilisez votre application en ligne.

Ce sentiment d'insécurité n'est pas justifié : chez ING, nous mettons tout en œuvre pour sécuriser nos canaux numériques. La sécurité, nous l'assurons ensemble. Vous trouverez ici un bref aperçu des mesures à prendre pour vous protéger.

Phishing (hammeçonage)

Le phishing consiste à vous envoyer un e-mail frauduleux contenant un lien permettant à des criminels d'essayer de voler vos données confidentielles. Ces données incluent notamment les codes numériques que vous créez avec votre lecteur de carte ING, votre code PIN ou le numéro de votre carte de débit ou de crédit. Ces criminels utilisent alors ces données pour effectuer des paiements au départ de votre compte.

Protégez-vous contre le phishing

- Les messages d'ING sont toujours personnalisés, sont rédigés dans votre propre langue et mentionnent votre nom et/ou votre prénom.
- Contrôlez l'expéditeur du message (adresse électronique). Les adresses e-mail d'ING se terminent toujours par ing.be ou ing.com.
- **ING ne vous demande jamais d'informations confidentielles**, comme votre code PIN ou les codes numériques de votre lecteur de carte. Ne transmettez jamais ces informations par e-mail ou par téléphone.
- Un lien dans un e-mail d'ING vous mènera toujours à ing.be
- Vérifiez le lien en déplaçant la souris sur le lien en question. Découvrez comment détecter les fraudes sur ing.be/fraude
- Ne vous connectez à la page d'accueil de Home'Bank ou de Business'Bank que via ing.be, et jamais via un lien dans un e-mail. Ne communiquez jamais non plus votre code secret!

Smishing

Les fraudeurs utilisent des SMS ou des messages WhatsApp et Facebook Messenger pour créer la panique et vous faire réagir précipitamment. Ces messages contiennent souvent un avertissement urgent... ...qui nous incitera à cliquer sur le lien.

Protégez-vous contre le smishing

Nous avons adapté nos directives pour faire face à ce type de fraude. Désormais **ING n'envoie plus de SMS avec des liens sur lesquels cliquer**. Si vous recevez un tel SMS, c'est qu'il ne provient pas d'ING, et vous devez donc absolument éviter de cliquer sur le lien.

Fraude sur les sites de seconde main

Supposons que vous vendiez des vêtements sur un site de seconde main. Un acheteur potentiel prend contact avec vous via une autre plateforme que celle du site de seconde main (par exemple WhatsApp ou Messenger). Cet acheteur vous demande de payer via une autre plateforme que celle du site de seconde main. Tout semble parfaitement normal... ... jusqu'à ce que vous vous aperceviez que votre compte bancaire a été pillé !

Protégez-vous contre la fraude sur les sites de seconde main

- Lisez toujours attentivement les consignes de sécurité du site de seconde main en question.
- N'acceptez jamais la proposition d'un acheteur potentiel de régler des transactions en dehors du site de seconde main.
- Ne payez jamais avec des moyens de paiement que vous ne connaissez pas.
- **Vous avez des doutes ? Mettez alors immédiatement fin à l'opération. Mieux vaut perdre un acheteur que tout votre argent.**

Restez informé(e) via ing.be/fraude
Nous publions régulièrement des informations sur les nouvelles formes de fraude. Découvrez sur ing.be/fraude comment reconnaître les fraudes et comment se protéger.

Vous avez été victime d'une fraude ?

- Bloquez votre carte bancaire via Card Stop en appelant au numéro **+32 70 344 344**.
- Appelez-nous immédiatement au **+32 2 464 60 02**. Nous sommes à votre disposition du lundi au vendredi de 8h à 22h et le samedi de 9h à 17h.
- Vous avez remarqué un mouvement suspect sur votre compte bancaire ? Envoyez-nous un e-mail via fraude@ing.be
- Vous avez reçu un message frauduleux au nom d'ING ? Envoyez-le nous à (phishing@ing.be).
- Pour les fraudes par carte de crédit : signalez l'achat frauduleux sur macarte.be

Vous disposez maintenant de toutes les informations nécessaires pour vous protéger. Installez aujoud'hui encore la nouvelle **ING banking-app**, via l'App Store ou Google Play.

Secured by ING

- ING met tout en œuvre pour assurer la sécurité de vos transactions en ligne et protéger votre vie privée.
- Vous effectuez ainsi vos opérations bancaires en ligne sur tous nos canaux digitaux dans un environnement entièrement sécurisé.

ING Belgique SA • Banque/Prêteur • Avenue Marnix 24, B-1000 Bruxelles • RPM Bruxelles • TVA : BE 0403.200.393 • BIC : BBRUBEBB • IBAN : BE45 3109 1560 2789 • www.ing.be • Contactez-nous via ing.be/contact • Courtier en assurances, inscrit à la FSMA sous le numéro 0403.200.393 • Éditeur responsable : Sali Salieski • Cours Saint-Michel 60, B-1040 Bruxelles – Z717142F • 11/2020