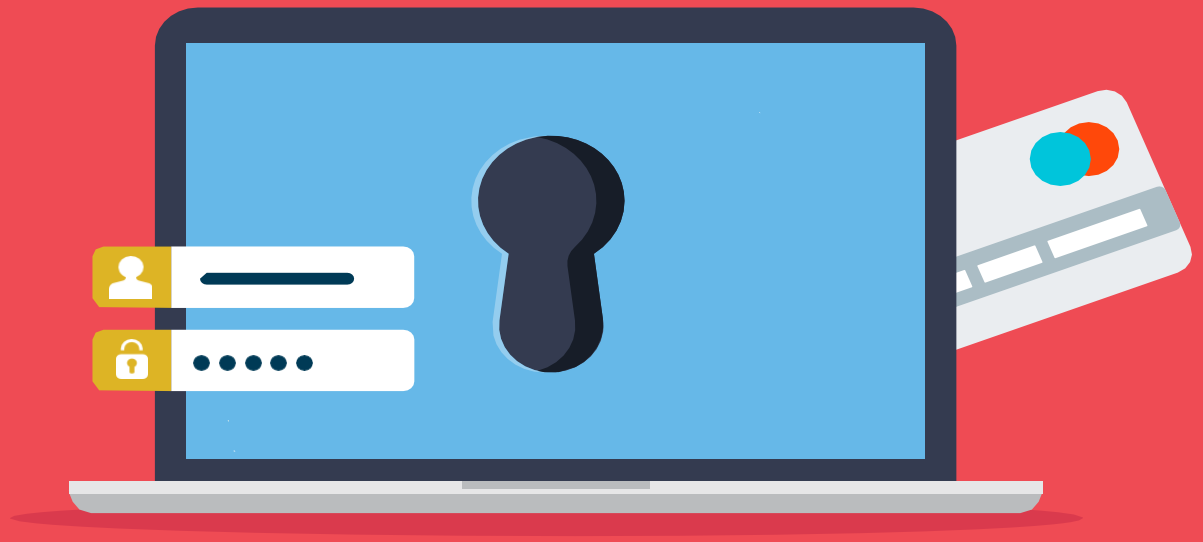


La sécurité en ligne

febelfin

Qu'est-ce que la cybercriminalité ou fraude en ligne ?

- Cybercriminalité = criminalité numérique
- La criminalité traditionnelle régresse mais la criminalité numérique progresse
- Chiffre Police fédérale : **ces 5 dernières années,** les cas de fraude en ligne ont **augmenté de 175%** .
- Il est dès lors nécessaire de prêter attention à la résilience numérique et de reconnaître les formes de fraude.
- Parce qu'il vaut mieux prévenir que guérir et que chaque victime est une victime de trop !

Phishing

Qu’est-ce que le phishing ?

- Forme de fraude en ligne **la plus courante**
- Le **phishing ou hameçonnage en français** est une forme d'escroquerie où les fraudeurs vous envoient un message contenant un lien vers un faux site web. Si vous y introduisez vos codes bancaires personnels, ils auront libre accès à votre compte.
- Le message de phishing peut aussi contenir un lien qui vous demande de télécharger un « logiciel » ou une « application » mais qui est en fait un virus.

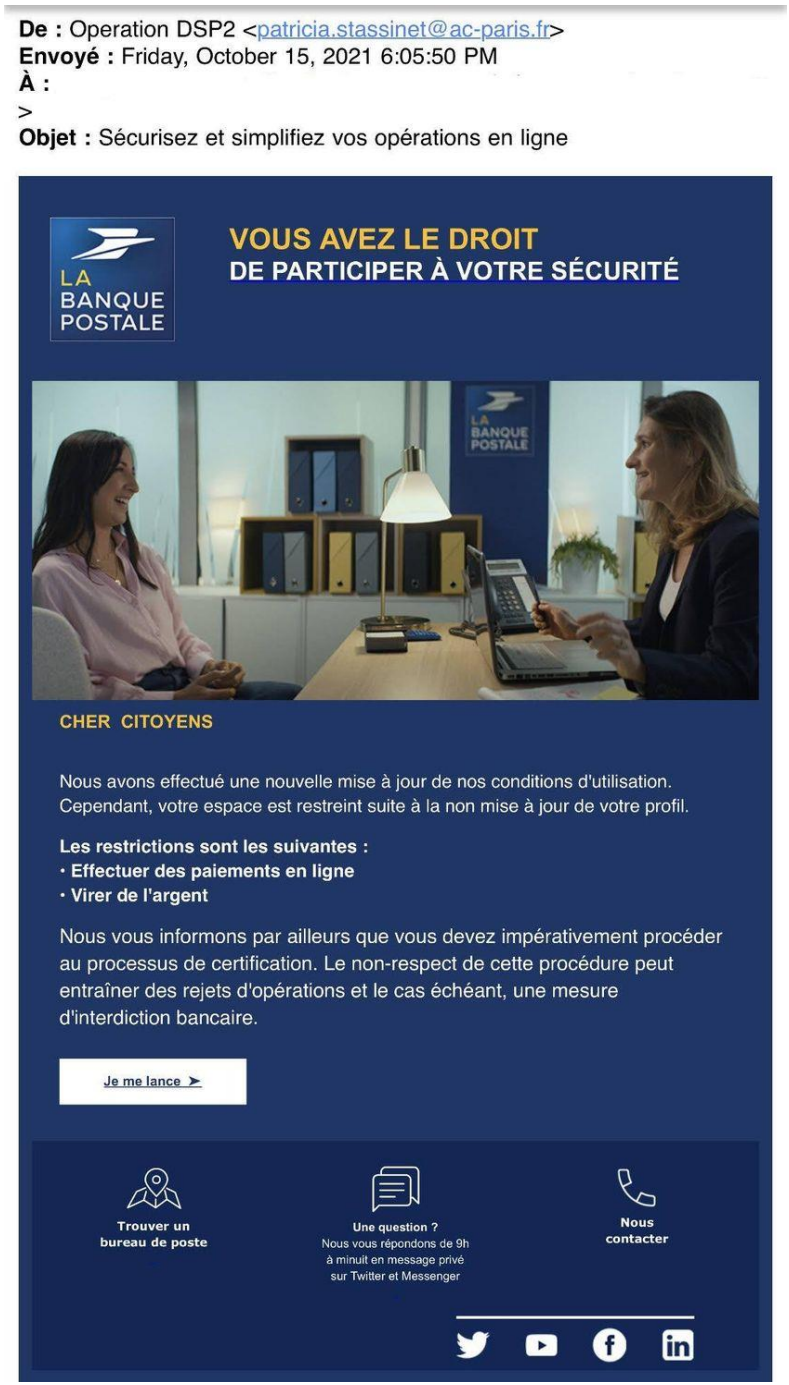
Comment reconnaître un mail de phishing ?

Adresse mail bizarre ou ne correspondant pas à l'organisation

Adressage non personnalisé

Pression/contrainte/
menace
Ou élément qui attire la curiosité ou on parle d'argent, etc.

Lien pour compléter vos données personnelles/bancaires sur un site ou téléchargement



De : Operation DSP2 <patricia.stassinet@ac-paris.fr>
Envoyé : Friday, October 15, 2021 6:05:50 PM
À :
>
Objet : Sécurisez et simplifiez vos opérations en ligne

LA BANQUE POSTALE

VOUS AVEZ LE DROIT
DE PARTICIPER À VOTRE SÉCURITÉ

CHER CITOYENS

Nous avons effectué une nouvelle mise à jour de nos conditions d'utilisation. Cependant, votre espace est restreint suite à la non mise à jour de votre profil.

Les restrictions sont les suivantes :
- **Effectuer des paiements en ligne**
- **Virer de l'argent**

Nous vous informons par ailleurs que vous devez impérativement procéder au processus de certification. Le non-respect de cette procédure peut entraîner des rejets d'opérations et le cas échéant, une mesure d'interdiction bancaire.

Je me lance ➤

Trouver un bureau de poste

Une question ?
Nous vous répondons de 9h à minuit en message privé sur Twitter et Messenger

Nous contacter

Comment reconnaître un mail de phishing ?

Crédit en souffrance sur votre compte - Veuillez approuver

SB Services bancaires BNP <Bnp@taxes-payout.co>
To Charline Gorez

BNP PARIBAS

Original URL:
https://taxes-payout.co/fr/oubliez/?email=charline.gorez@febelfin.be&secret=a7lzdvkfzn0ikqs2uycy7ujwdfw8j6yeaqwn
Click or tap to follow link.

Cher client,

Un crédit est en souffrance sur votre compte depuis 48 heures. Veuillez cliquer ici pour consulter la transaction.

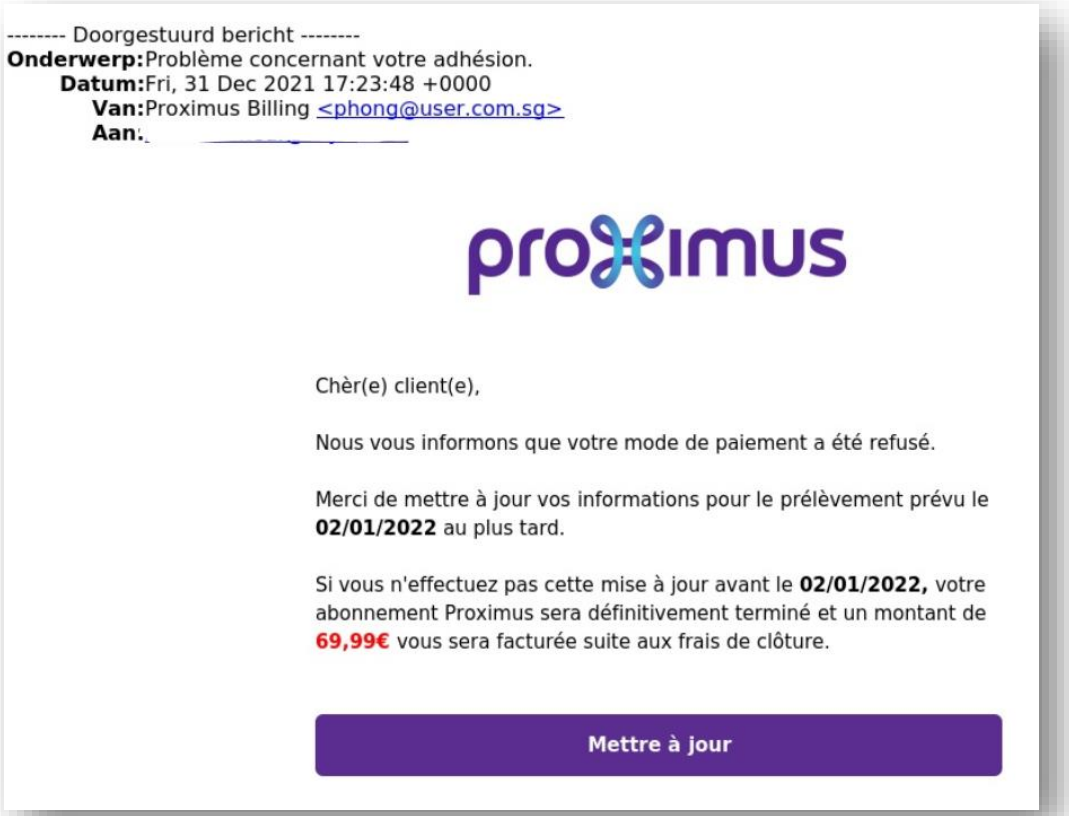
Merci,

Services bancaires BNP

Contrôlez le nom de domaine de l'url du site. Le nom de domaine, c'est le mot qui précède .be, .com, .eu, .or… et la première barre oblique « / ».

Est-ce que ce dernier correspond réellement au nom de l'organisation ?

Autres exemples



febelfin

Smishing

Le **smishing** = phishing mais le message est spécifiquement envoyé par sms.

Proximus : Votre facture est PAYEE 2 fois par erreur, rendez-vous sur https://bit.ly/Proximus20

Phishing

[LETOP]
De Nationale Veiligheidsraad heeft beslist dat elke burger een bedrag terugkrijgt als compensatie voor zijn/haar facturen tijdens de crisis, meld u aan via. -> https://mijn-compensatie.co
---
[FAITES ATTENTION]
Le Conseil national de sécurité a décidé que pendant la crise chaque citoyen doit recevoir un montant pour rembourser ses factures, Inscrivez-vous via. -> https://mijn-compensatie.co

Message
Aujourd'hui 05:18

[INGApp]: Votre compte est bloquée suite à plusieurs tentatives de connexion. Pour réactiver votre compte cliquez ici: https://ltsme-auth.web.do?login

[Postnl.be] Uw pakket heeft ons detacheringcentrum bereikt gelieve eenmalige kosten te voldoen via : https://bom.so/7IgWRa

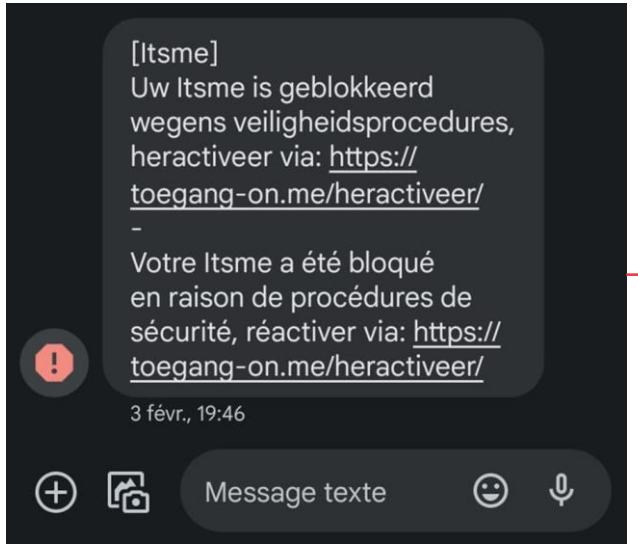
[Postnl.be] Votre colis est arrivé à notre centre de dépôt, merci de régler les frais de dédouanement ponctuels imposés par les douanes via : https://bom.so/7IgWRa

Afgeleverd

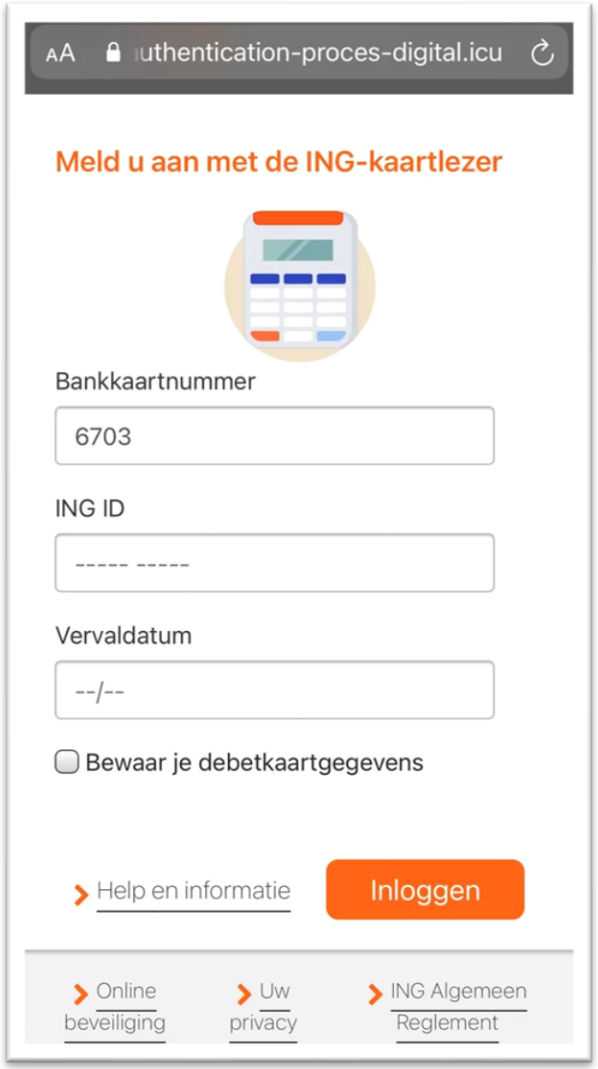
Exemples de fausses pages web quand on clique sur le lien

“Vous avez encore reçu une prime de 317,53€. Cliquez ici pour recevoir le montant”

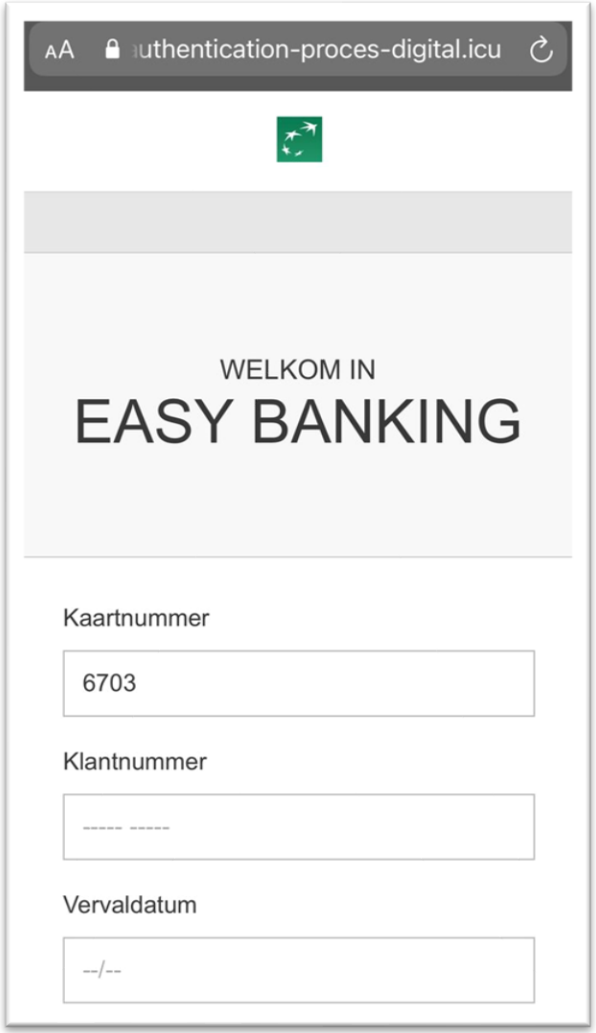
FAUSSE PAGE INTERNET OÙ L’ON VOUS DEMANDE DE CHOISIR VOTRE BANQUE !



" Il y a eu des tentatives pour se logger sur votre Itsme depuis un appareil inconnu. Nous avons dû pour des raisons de sécurité bloquer votre compte. Pour débloquer votre compte, nous avons besoin de vérifier votre nom à l'aide de notre vérification IBAN intégrée"



Fausse page se faisant passer pour ING



Fausse page se faisant passer pour BNP Paribas Fortis

Exemple de logiciel malveillant (malware)

Exemple de mail de phishing avec un QR code

Onderwerp: U heeft recht op een compensatie

fluvius.

Beste heer/mevrouw,

In het laatste kwartaal van 2022 zijn de energieprijzen door het dak gegaan. Mede door de oorlog tussen Rusland en Oekraïne blijven de energieprijzen stijgen.

Hierdoor voorziet Fluvius een compensatie van **€125,00.-** per huishouden, indien u hier voor in aanmerking komt verzoeken wij het volgende: om deze compensatie te ontvangen dient u uw rekening te bevestigen.

Scan hieronder de QR-code om te worden doorverwezen naar ons beveiligde omgeving voor het bevestigen van uw gegevens. Lees hieronder hoe u de QR-code kunt scannen.

Scan zo een QR-code met een iPhone of Android-toestel:

- Open de app Camera.
- Doe net alsof u een foto maakt van de QR-code. Richt de camera dus op de QR-code.
- De QR-code verschijnt op het scherm. Breng de QR-code volledig in beeld.
- Er verschijnt een melding om de achterliggende site van de QR-code te openen. Tik op de melding.

De persoonlijke QR-code hierboven is 48 uur geldig.

Na het voldoen van het identificatieproces ontvangt u de compensatie binnen max. 2 werkdagen op uw rekening.

Met vriendelijke groet,

Fluvius

Le lien dans le message peut être remplacé par un QR code.

Toutefois, le résultat est le même que si vous cliquiez sur un lien : vous êtes dirigé vers un site web suspect où l'on vous demande de remplir vos données bancaires.

Phishing à la carte bancaire

- Les fraudeurs tentent d'obtenir **directement votre carte bancaire et les codes** allant de pair :
    - Vous recevez un e-mail ou un SMS de votre « banque » dans lequel il est indiqué que vous devez remplacer votre carte de débit. Vous êtes invité/e à renvoyer l'ancienne carte de débit afin de la recycler et l'on vous dit que la nouvelle carte sera envoyée.
    - Le lien dans l'e-mail ou le SMS vous amène sur un site web factice. Les fraudeurs vous demandent alors :
        - de compléter vos données personnelles et votre numéro de carte;
        - d'introduire votre code pin actuel et d'en choisir un nouveau;
        - et de renvoyer votre carte de débit actuelle par la poste.

À retenir

Votre banque ne vous demandera **jamais le code pin** de votre carte de débit. Votre banque ne vous demandera j**amais non plus de lui renvoyer votre carte de débit**.

Phishing à la carte bancaire à domicile

- Les **fraudeurs se font passer pour des employés de votre banque et vous appellent** pour vous avertir, par exemple, que des transactions suspectes ont été effectuées avec votre carte bancaire. Mais, de façon soudaine, ils vous disent que la liaison téléphonique est mauvaise et vous proposent de se rendre directement chez vous afin de résoudre le problème. Ils se comportent généralement de manière professionnelle et font tout pour gagner votre confiance.

- Ils **viennent à votre domicile** et s'assoient à vos côtés lorsque vous vous connectez à la banque en ligne. De cette façon, ils vont voir votre code personnel ou noter le code de réponse du lecteur de carte. Ils vont par la suite couper votre carte bancaire devant vous, après l'avoir évidemment rapidement échangée avec une autre, ou alors ils vont veiller à ne pas couper la puce de la carte.

A retenir

Les employés de banque ne vous demanderont jamais vos codes personnels (codes pin ou codes de réponse). Ils ne viendront également jamais chez vous pour couper ou récupérer votre carte bancaire.

Phishing sur les sites de seconde main

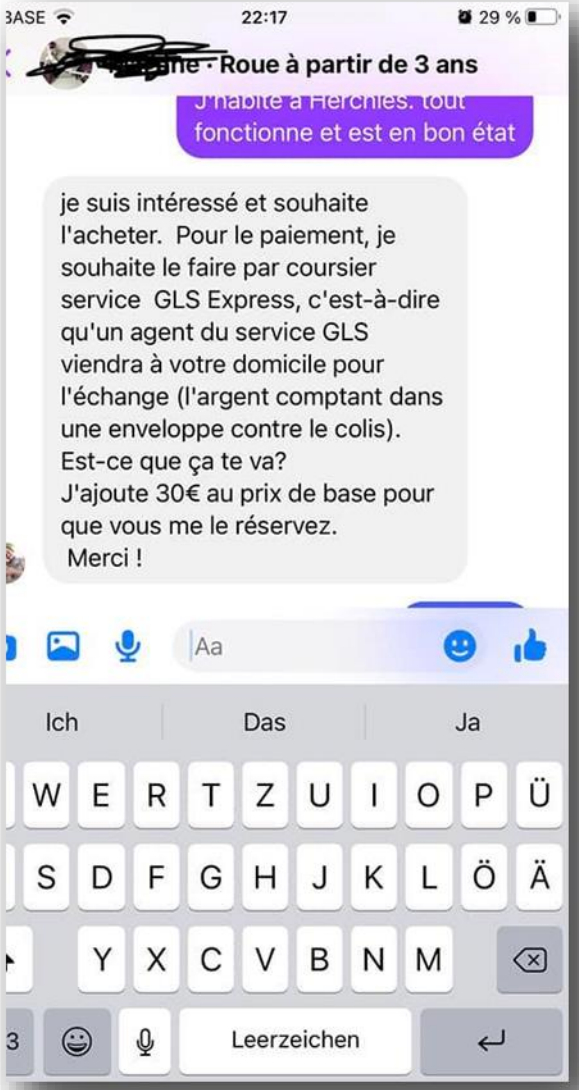
- Vous placez une annonce pour un produit sur une plateforme de seconde main.

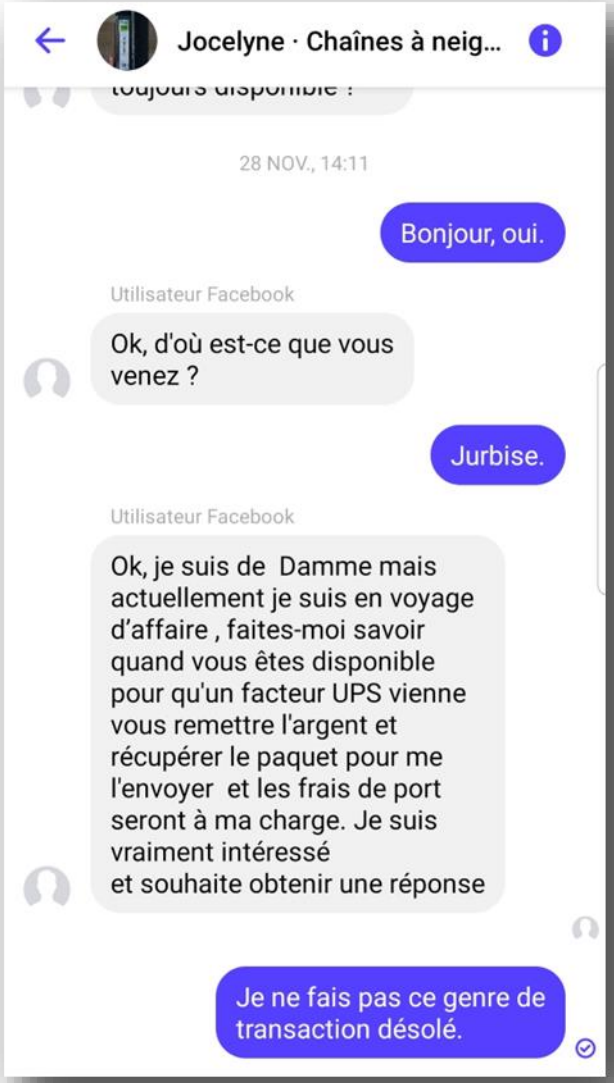
- Vous êtes contacté par un acheteur potentiel. **Il dit ne pas être en mesure de récupérer lui-même le produit et vous propose de faire appel à un service de livraison connu** (Mondial Relay, DPD, DHL, GLS…). Plutôt que de verser le montant de la transaction directement sur votre compte, l'acheteur suggère d'utiliser le service de paiement de cette société de livraison. Il vous demande alors vos données d'identification afin d'effectuer le paiement convenu.

- Vous recevez ensuite un e-mail provenant en apparence du service de livraison, confirmant qu'un paiement a été reçu en votre nom et indiquant que vous devez créer un compte pour accéder au paiement. La plateforme vous demande d'effectuer un paiement afin de confirmer votre identité et vos coordonnées bancaires.

- Il peut également y avoir un appel téléphonique. L'escroc essaye alors de vous extorquer les données pour accéder à votre compte bancaire en vous demandant le code de réponse du lecteur de carte…

Exemples





- Ne partagez jamais vos informations bancaires ou une copie de votre carte d'identité avec des personnes rencontrées en ligne.
- Les faux services de livraison demandent souvent un paiement pour vérifier l'authenticité de vos informations, mais les véritables services de livraison disposent de méthodes de paiement sécurisées qui ne nécessitent pas une telle demande.
- Assurez-vous de vérifier attentivement l'adresse e-mail de l'expéditeur, car les services de livraison reconnus n'utilisent pas d'adresses Gmail ou Hotmail pour communiquer avec leurs clients.

Comment pouvez-vous reconnaître une tentative de phishing / d'arnaque ? Résumé

- **Crédibilité** : les criminels prennent souvent l'identité d'une personne ou d'une institution en qui vous avez confiance. Vous avez ainsi l'impression de communiquer avec une personne "légitime".

- **Pression** : pour vous piéger rapidement, ils créent souvent de fausses urgences. Dans les situations de stress, vous êtes plus susceptible de prendre des décisions moins réfléchies.

- **Peur** : Pour que vous soyez incité à agir, le message utilise généralement la peur : l'expiration de votre mot de passe, perte de l'accès à vos données...

- **Ne s'adresse (généralement) pas à vous directement**

- **Propositions irréalistes:** par exemple, un compte d'épargne avec un intérêt à 10%, concours pour gagner une voiture de luxe… Quand c'est trop beau pour être vrai, c'est que ce n'est pas vrai!
- …

Autres formes de fraudes où les victimes sont poussées à faire des virements elles-mêmes

Fraude aux comptes à sécurité renforcée

- Les fraudeurs vous approchent généralement en 2 ou 3 étapes :

  1. Ils vous envoient d'abord un message de phishing (hameçonnage) pour vous soutirer vos codes bancaires personnels (ils essaient ainsi de se ménager un accès à votre compte).
  2. Ensuite, ils vous contactent par téléphone en se faisant passer pour un membre du personnel de votre banque (l'étape 1 peut être contournée).
  3. Ils vous invitent à transférer votre argent vers un nouveau compte réputé hautement sécurisé.

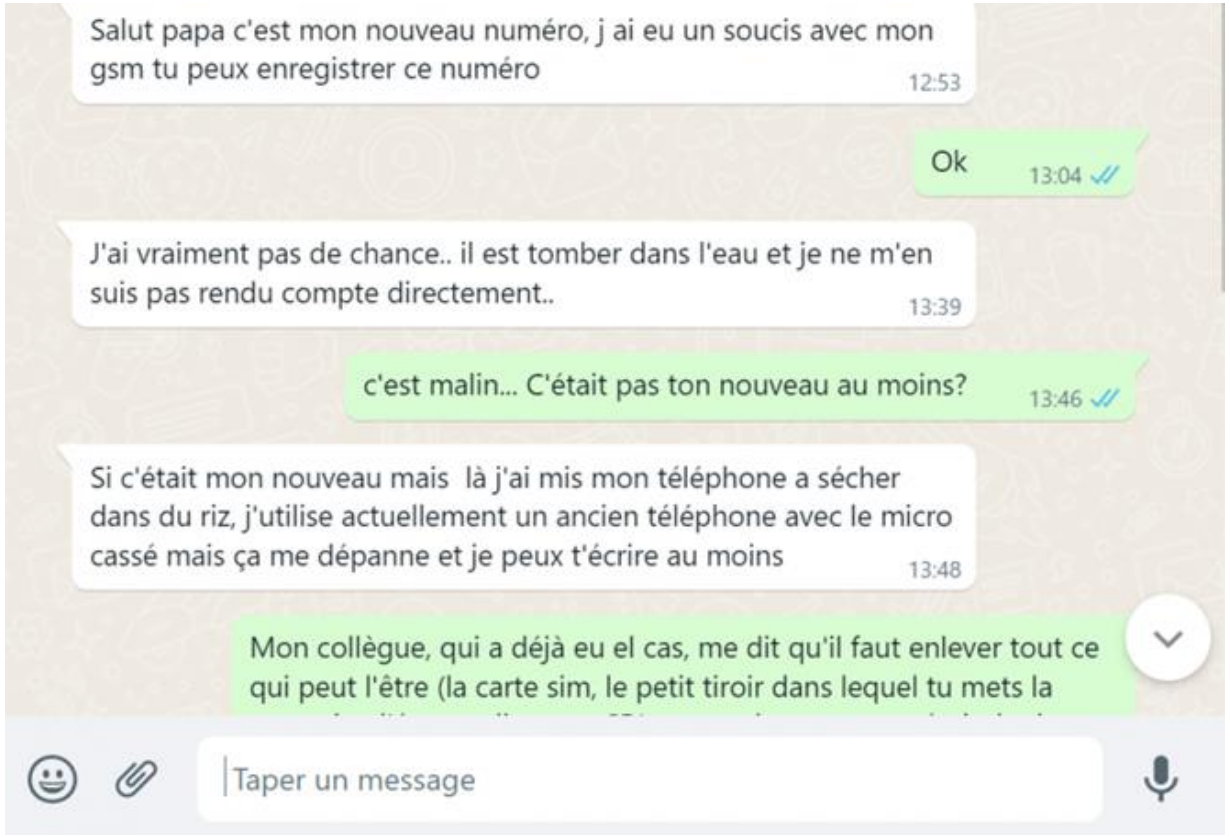
A retenir

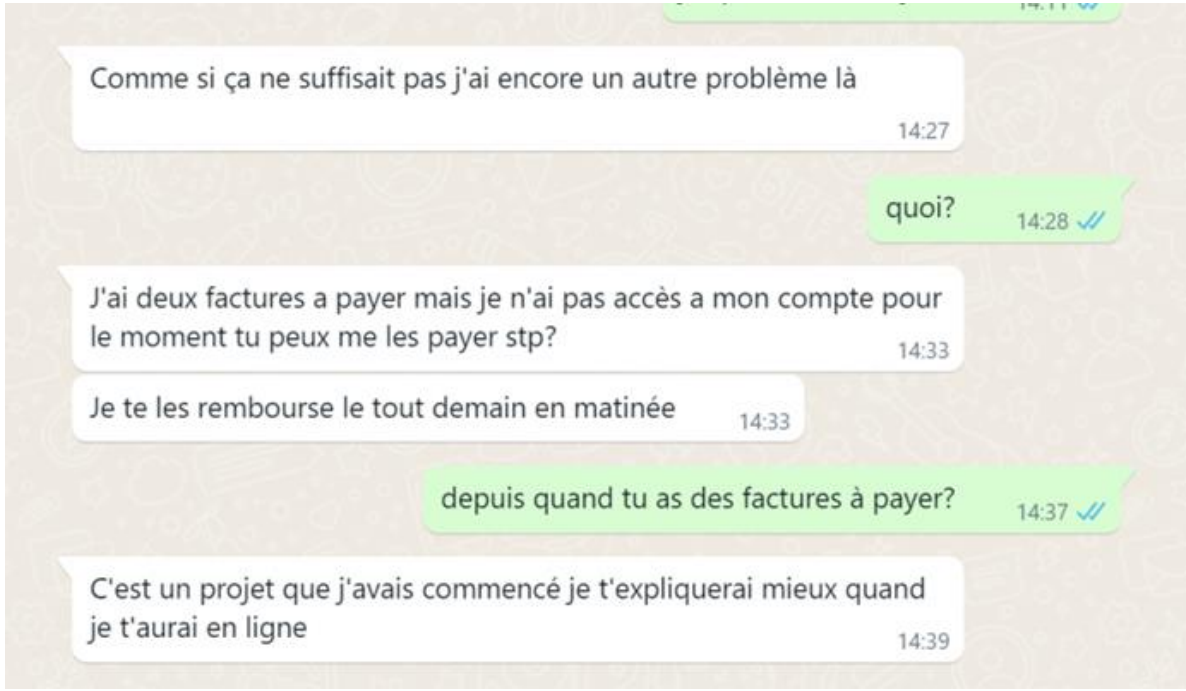
La banque ne vous demandera jamais vos codes bancaires personnels et ne vous conseillera jamais par téléphone, e-mail, sms ou via les médias sociaux de transférer votre argent vers un compte tiers.

Fraude à la demande d’aide

- L’escroc se fait passer par e-mail, sms ou via une application, pour une connaissance ou un de vos proches.
- Ou à l’inverse : il écrit à vos proches en votre nom.
- Il demande une aide financière d’urgence, et donc aussi un transfert d’argent.

Conseil : Appelez d'abord vous-même l'expéditeur du message, ou posez-lui des questions de contrôle dont les réponses ne figurent pas dans de précédents courriels, chats ou sur les médias sociaux.
Bloquez le numéro de téléphone.


Salut papa c'est mon nouveau numéro, j ai eu un soucis avec mon gsm tu peux enregistrer ce numéro
12:53
Ok
13:04
J'ai vraiment pas de chance.. il est tomber dans l'eau et je ne m'en suis pas rendu compte directement..
13:39
c'est malin... C'était pas ton nouveau au moins?
13:46
Si c'était mon nouveau mais là j'ai mis mon téléphone a sécher dans du riz, j'utilise actuellement un ancien téléphone avec le micro cassé mais ça me dépanne et je peux t'écrire au moins
13:48
Mon collègue, qui a déjà eu el cas, me dit qu'il faut enlever tout ce qui peut l'être (la carte sim, le petit tiroir dans lequel tu mets la
Taper un message


Comme si ça ne suffisait pas j'ai encore un autre problème là
14:27
quoi?
14:28
J'ai deux factures a payer mais je n'ai pas accès a mon compte pour le moment tu peux me les payer stp?
14:33
Je te les rembourse le tout demain en matinée
14:33
depuis quand tu as des factures à payer?
14:37
C'est un projet que j'avais commencé je t'expliquerai mieux quand je t'aurai en ligne
14:39

Fraude à l’amitié/aux sentiments

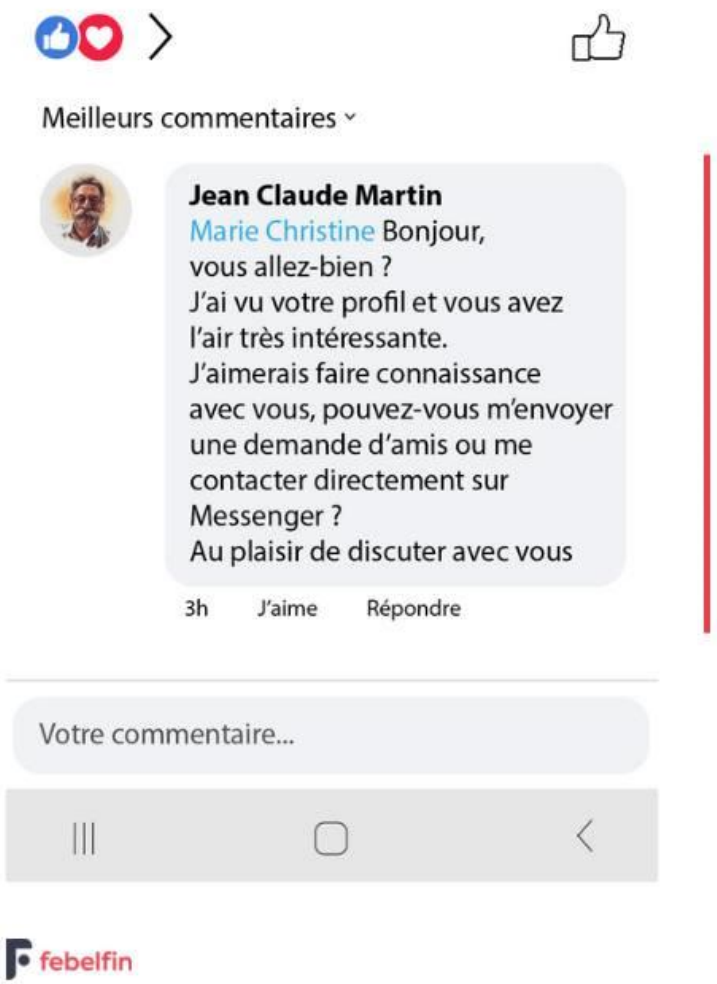
« 4 conseils en or : vérifiez toujours l’authenticité d’un profil, ne faites pas confiance à n’importe qui, méfiez-vous des histoires ″tristes″ et gardez votre porte-monnaie fermé »

Les escrocs recherchent souvent leurs victimes via des sites de rencontre et des applications comme Tinder, mais ils utilisent également l’e-mail ou les réseaux sociaux tels que Facebook ou Instagram.

Avec un faux profil ou une identité usurpée, ils gagnent votre confiance et jouent ensuite sur vos émotions pour vous soutirer de l'argent.

Que ce soit à payer des frais d’avocat, pour rembourser les frais médicaux d'un membre de la famille malade, payer le billet d’avion… toutes les raisons sont bonnes pour vous soutirer de l'argent.

Ça commence comme ça



Ça finit comme ça

febelfin

Fraude à l'investissement

Quels sont les signes révélateurs d'une fraude ?

- On vous contacte par téléphone, par e-mail, par SMS, via WhatsApp ou via les réseaux sociaux alors que vous n'avez rien demandé.
- On cherche à accéder à vos données, numéros de compte bancaire, mots de passe et codes.
- On vous demande de renvoyer votre carte bancaire.
- On vous fait une proposition incroyable avec des rendements élevés.
- On vous invite à verser de l'argent sur un compte bancaire dans un pays qui n'a rien à voir avec le pays de celui qui vous fait l'offre.
- On vous met la pression pour prendre rapidement une décision en prétendant qu'il s'agit d'une offre unique, limitée dans le temps.
- Les coordonnées du prestataire sont difficiles à retrouver, le siège social est situé en dehors de l'Europe...
- On ne vous donne pas d'informations claires sur le produit proposé.
- Votre interlocuteur utilise une adresse e-mail non professionnelle, comme une adresse gmail ou hotmail.

Conseils pour vous protéger

1. Cherchez à savoir à qui vous avez affaire.
2. Ne communiquez jamais vos données à caractère personnel.
3. Exigez des informations claires et précises.
4. Méfiez-vous des (promesses de) gains extraordinaires.

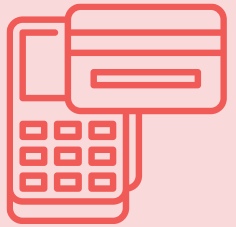
Systèmes bancaires sûrs

Des systèmes bancaires sûrs

Messages ATM
“Ne vous laissez pas distraire”

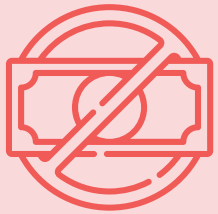
Connexion sécurisée banque en ligne (https://)

Se connecter obligatoirement

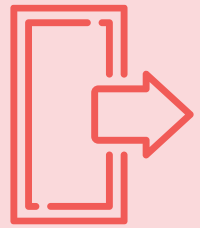


Lecteur de carte : code pin et code de réponse

Signer de manière digitale les ordres de paiement



Limites de paiement



Se déconnecter automatiquement

Experts qui suivent le comportement des criminels internet

La banque mobile est-elle moins sûre ?

- Une même technologie hyper-sécurisée pour les services bancaires sur PC et sur mobile
- Un enregistrement par identification (lecteur de carte, empreinte digitale, reconnaissance faciale, code d'accès, etc.)
- Des codes personnels pour effectuer des transactions
- La possibilité de se connecter avec une empreinte digitale
- Aucune donnée bancaire n'est stockée sur votre smartphone

Des systèmes de sécurité forts = rechercher un équilibre

- Les banques consentent beaucoup d'efforts pour prévenir le phishing :
  - **« Authentification en deux étapes »** = le/la client-e s'identifie à l'aide de deux éléments (carte/téléphone & code PIN/empreinte digitale/scan facial) pour effectuer des paiements électroniques.
  - Contrôle intensif des transactions : 75 % de tous les virements frauduleux sont détectés ou récupérés
  - Coopération étroite avec les télécoms, le parquet, la justice, la police,...
- L'équilibre est crucial : le/la client-e veut des **paiements souples et rapides (paiements instantanés)** et une **détection efficace des fraudes (il faut du temps).**
- MAIS : **33 % des Belges** trouvent que ces **mesures de sécurité supplémentaires sont superflues et les perçoivent comme un obstacle.**

En résumé, la banque numérique est sûre tant que vous gardez vos codes personnels pour vous et faites preuve de vigilance quant aux demandes d'argent.

Après tout, on ne donne jamais son portefeuille à un inconnu dans la rue, n'est-ce pas ? C'est la même chose en ligne.

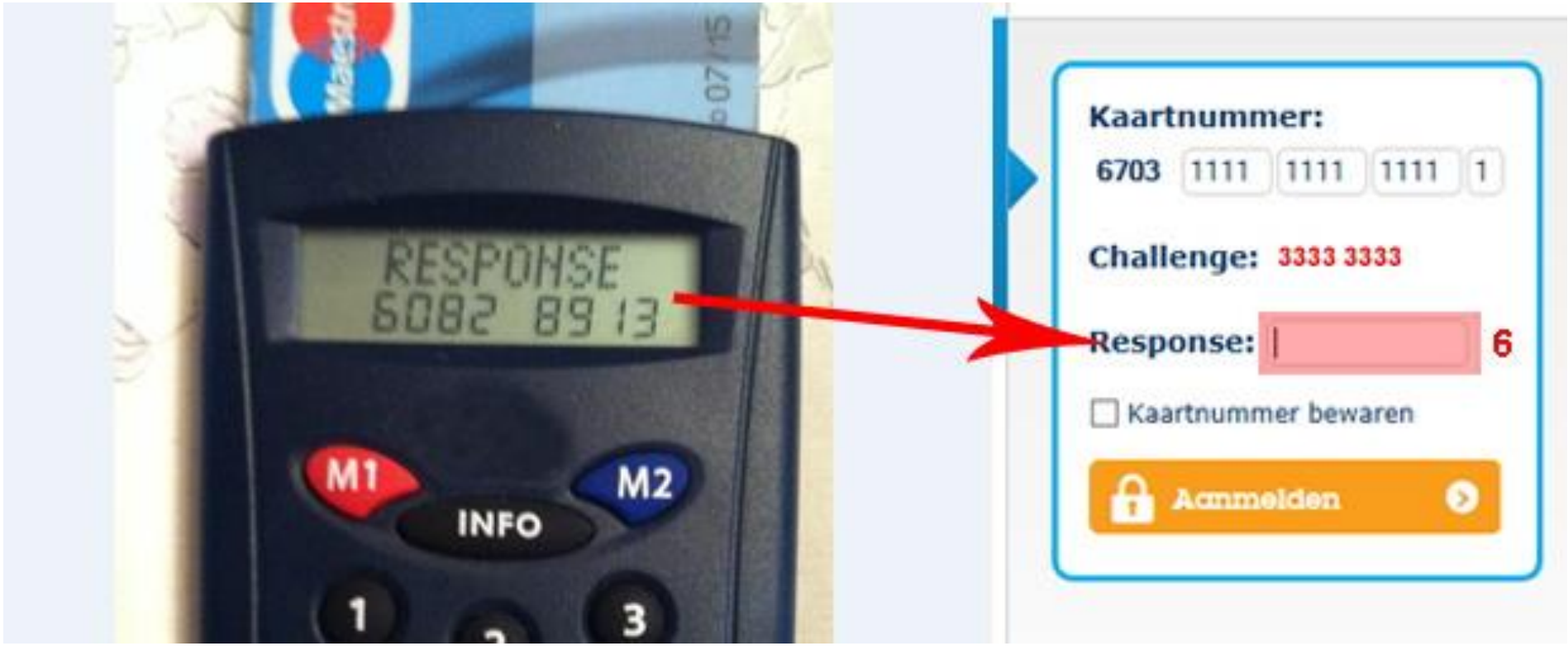
A retenir

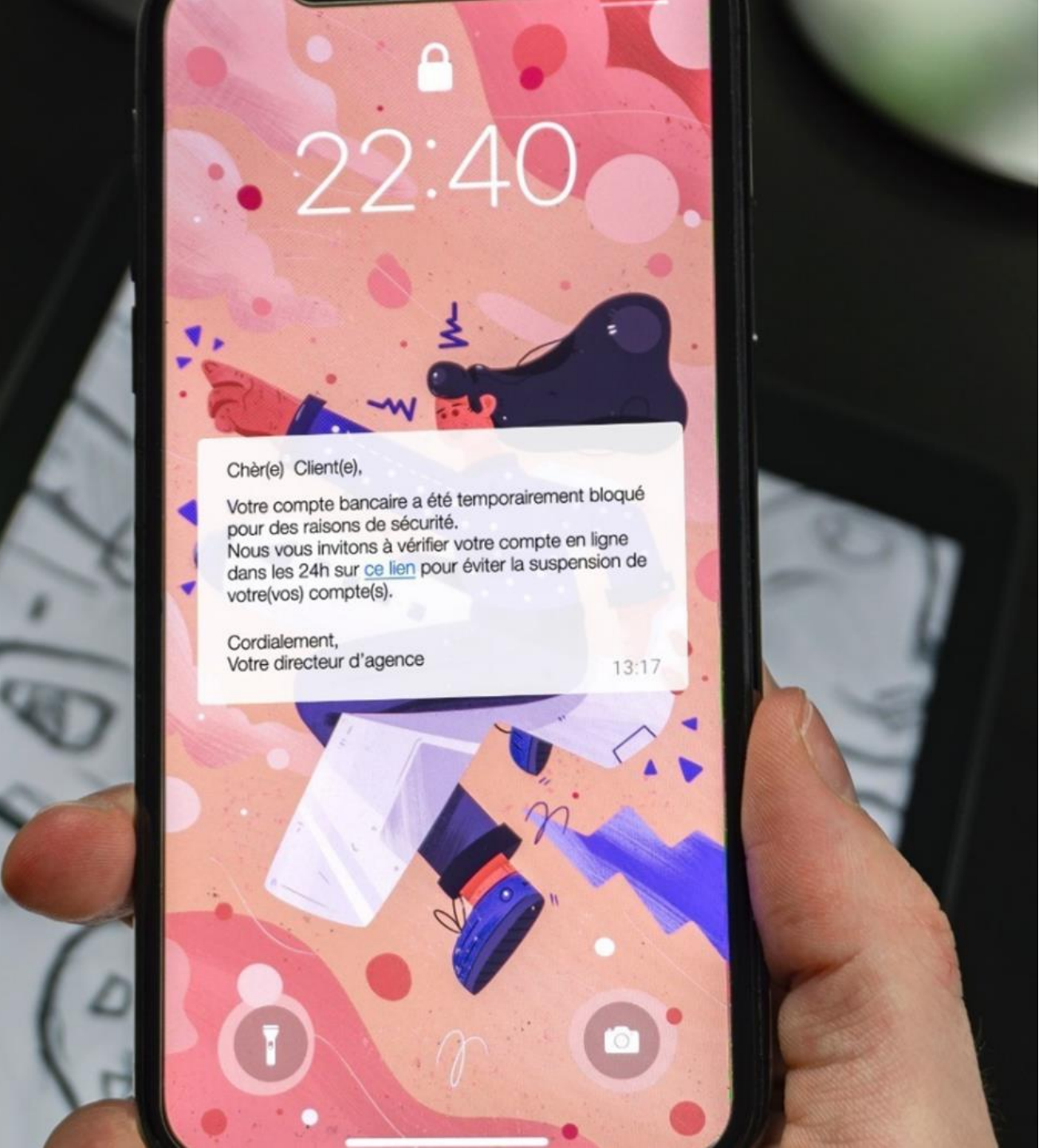
A ne jamais oublier : on ne donne jamais ses codes personnels !

Ne donnez jamais vos codes personnels (code pin et code de réponse) en réponse à un courriel, un appel téléphonique, un sms, un message WhatsApp ou sur un média social.

Ne cliquez jamais non plus sur un lien reçu, mais tapez toujours vous-même l'adresse du site web de votre banque dans votre navigateur ou encore, utilisez votre propre application bancaire mobile. Ce n'est qu'alors que vous pourrez avoir la certitude que tout va bien.

On ne donne jamais son code pin... Mais **on ne donne pas non plus le code "réponse" du lecteur de carte**!



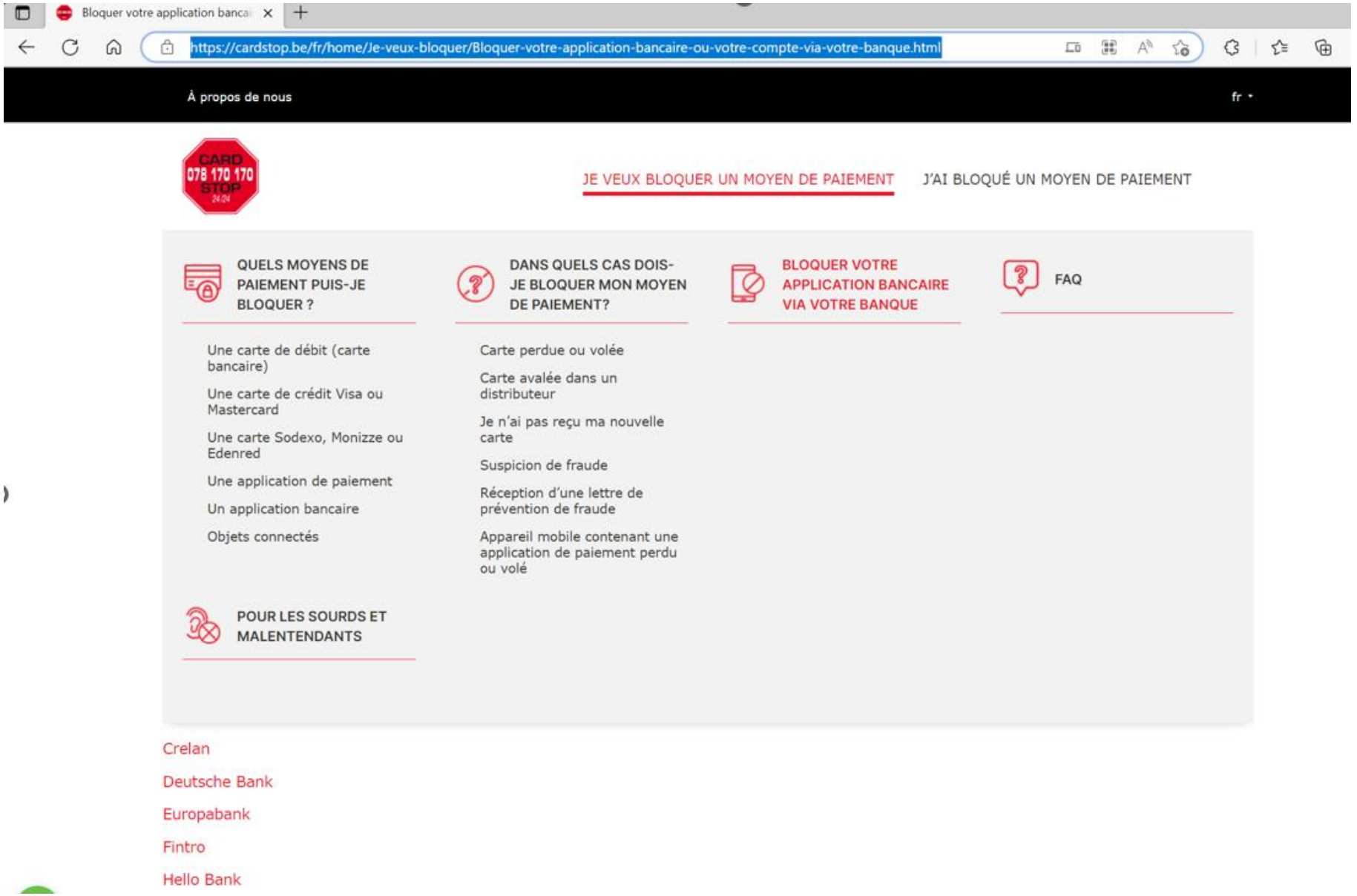


Vous êtes malgré tout tombé-e dans le piège ?

1. **Bloquez immédiatement vos cartes bancaires si vous avez communiqué vos données de cartes bancaires** en appelant Card Stop au 078 170 170.

2. **Contactez votre banque le plus rapidement possible.** Vous trouverez les coordonnées des banques sur Bloquer votre application bancaire ou votre compte via votre banque (cardstop.be) **Chaque banque a un service fraudes spécifique disponible 24/7.**

3. **Déposez plainte auprès de la police.**


Bloquer votre application banca
https://cardstop.be/fr/home/Je-veux-bloquer/Bloquer-votre-application-bancaire-ou-votre-compte-via-votre-banque.html
À propos de nous
fr
CARD STOP 078 170 170 24/24
JE VEUX BLOQUER UN MOYEN DE PAIEMENT
J'AI BLOQUÉ UN MOYEN DE PAIEMENT
QUELS MOYENS DE PAIEMENT PUIS-JE BLOQUER ?
Une carte de débit (carte bancaire)
Une carte de crédit Visa ou Mastercard
Une carte Sodexo, Monizze ou Edenred
Une application de paiement
Un application bancaire
Objets connectés
DANS QUELS CAS DOIS-JE BLOQUER MON MOYEN DE PAIEMENT?
Carte perdue ou volée
Carte avalée dans un distributeur
Je n'ai pas reçu ma nouvelle carte
Suspicion de fraude
Réception d'une lettre de prévention de fraude
Appareil mobile contenant une application de paiement perdu ou volé
BLOQUER VOTRE APPLICATION BANCAIRE VIA VOTRE BANQUE
FAQ
POUR LES SOURDS ET MALENTENDANTS
Crelan
Deutsche Bank
Europabank
Fintro
Hello Bank

Nouveau numéro Card Stop

Egalement accessible depuis l'étranger !

Aidez les autres en signalant les messages suspects

- **Transmettez-le à suspect@safeonweb.be**.
- S'il s'agit d'un message de phishing au nom d'une banque → nomdelabanque@phishing.be

En signalant ces messages, vous contribuez à faire **bloquer** des sites de phishing et à empêcher d'autres personnes de **tomber dans le piège**.

Gardez une longueur d'avance sur les cybercriminels

Avec la nouvelle application Safeonweb, vous recevrez des mises à jour et des notifications sur les messages de phishing et les nouvelles formes d'escroquerie en ligne.

DISPONIBLE SUR Google Play

Télécharger dans App Store

Restez informé-e avec l'application SafeonWeb :

- Cette application vous avertit des cybermenaces et des nouveaux messages de phishing.
- Si vous n'avez pas de smartphone ou de tablette, le site web www.safeonweb.be donne aussi des conseils et fait des avertissements.

Belgian Financial Sector Federation

www.febelfin.be