Sécurité en ligne : protégez-vous contre la fraude

Découvrez notre brochure dédiée à la sécurité en ligne.

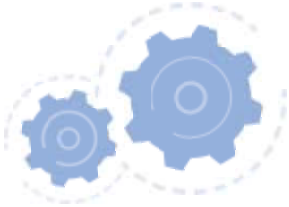
Apprenez les meilleures pratiques pour reconnaître une tentative de fraude, préserver vos données confidentielles et utiliser les services bancaires en toute confiance. Que vous soyez novice ou expérimenté, soyez maître de votre sécurité numérique !

RÉGION DE BRUXELLES-CAPITALE

paradigm .brussels

febelfin

Table des matières



Les systèmes bancaires sont sécurisés

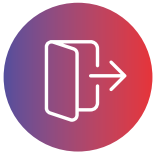
Les services bancaires numériques intègrent des mécanismes de sécurité, ainsi que des vérifications et des contrôles pour prévenir et détecter les fraudes éventuelles.

> Les opérations bancaires en ligne et mobiles se font toujours via une **connexion sécurisée.**

> Pour accéder à la banque numérique, **votre banque vous demandera toujours de vous identifier de manière sécurisée à l'aide de deux éléments ou plus appartenant aux catégories suivantes** : quelque chose que seul l'utilisateur connaît (code secret) ; quelque chose que seul l'utilisateur possède (carte bancaire ou téléphone portable) ; quelque chose que l'utilisateur est (reconnaissance faciale ou empreinte digitale). Vous utilisez généralement l'un de ces facteurs, souvent un mot de passe, pour prouver qui vous êtes. Mais pour la banque en ligne, **il est obligatoire d'en utiliser deux ou plus : c'est ce qu'on appelle «l'authentification forte du client»**.

> Votre banque applique des **limites de paiement**. Vous ne pouvez donc pas dépenser plus qu'un certain montant par jour.

> Si la banque remarque **un ordre de paiement suspect**, elle effectue d'abord un certain nombre de contrôles supplémentaires avant d'exécuter le virement.



> Vous êtes **automatiquement déconnecté de la banque en ligne** si aucune activité n'a été effectuée pendant une certaine période.

> **La technologie hypersécurisée des services bancaires** sur PC est équivalente à celle sur les smartphones et tablettes. De plus, aucune donnée bancaire n'est stockée sur votre smartphone.

Comment se protéger de la fraude en ligne ?

Ne communiquez jamais vos codes

De quels codes parle-t-on ?

> **Votre code PIN** : le code associé à votre carte bancaire.

> Le **code** pour entrer dans votre **application bancaire**.

> Les **réponses du lecteur de carte** qui constituent une authentification forte.

Votre banque et d'autres organisations dignes de confiance ne vous demanderont jamais de communiquer vos codes.

Ne signez jamais une transaction via itsme ou votre lecteur de carte que vous n'avez pas initiée vous-même.

Voici un lecteur de carte bancaire :

Numéro de carte :

6703

Challenge : 1111 1111

Réponse :

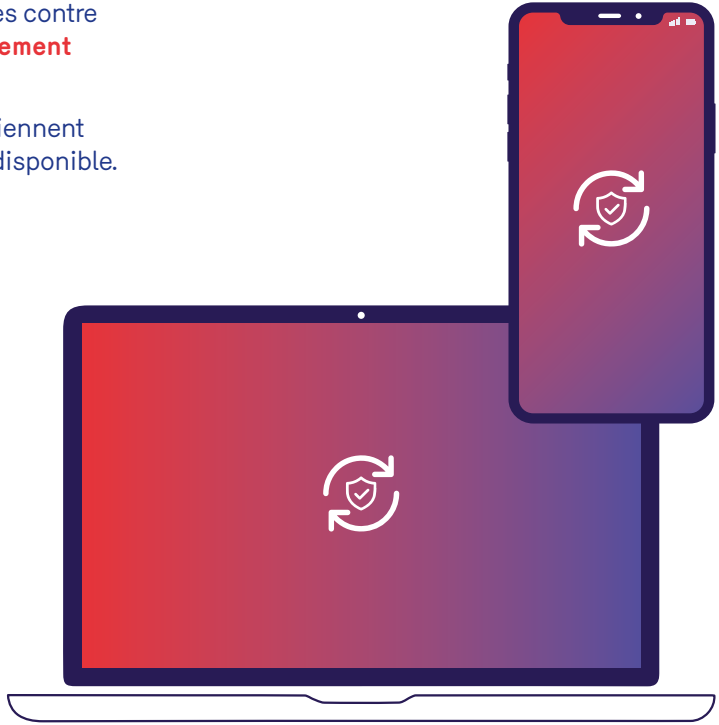
Enregistrer

On ne donne JAMAIS son code PIN...
Mais on ne donne pas non plus le code « réponse » du lecteur de carte !

Installez les mises à jour de vos appareils

Il est important de protéger vos données contre les cybercriminels **en mettant régulièrement à jour vos appareils.**

Généralement, vos appareils vous préviennent quand une mise à jour de sécurité est disponible.



Réfléchissez avant de vous précipiter

Méfiez-vous du caractère « urgent » d'une demande.

L'urgence est un prétexte souvent utilisé par les fraudeurs pour créer un sentiment de panique chez leurs victimes.

Ils veulent vous faire agir rapidement, sans vous laisser le temps de poser des questions et de réaliser qu'il s'agit d'une escroquerie.

Si vous pensez être victime d'une tentative de fraude, prenez le temps d'analyser la demande et renseignez-vous en cherchant les coordonnées de l'organisme mentionné dans le message et en le contactant vous-même.

N'utilisez pas les numéros de téléphone, adresses e-mail ou adresses web trouvés dans le message.

En cas de doute, arrêtez tout contact et toute transaction. Signalez le message à **suspect@safeonweb.be** et supprimez-le.

Utilisez une connexion sécurisée lors de la saisie d'informations sensibles

> Utilisez une connexion sécurisée

Prenez des précautions lorsque vous utilisez un réseau Wi-Fi gratuit en dehors de votre domicile.

On retrouve des hotspots Wi-Fi gratuits dans de nombreux lieux publics. Bien que pratiques, ces réseaux sont accessibles à tout le monde, ce qui augmente le risque de cybercriminalité.

Pour minimiser ce risque, évitez donc de vous connecter à votre banque en ligne et mobile via un Wi-Fi public et utilisez plutôt le réseau 3G, 4G ou 5G sur votre téléphone et sur votre ordinateur ou tablette via le partage de connexion.

Chez vous, vous pouvez utiliser votre propre Wi-Fi en toute sécurité.

> Consultez des sites internet sécurisés

Vérifiez également que la connexion est sécurisée en regardant l'URL, c'est-à-dire l'adresse web qui apparaît dans la barre de navigation (en haut de votre navigateur). Celui-ci doit impérativement commencer par **« https:// »**. Le **« s »** dans « https » signifie que la connexion est sécurisée. Vous pouvez aussi voir un petit cadenas 🔒 à gauche de l'adresse du site.

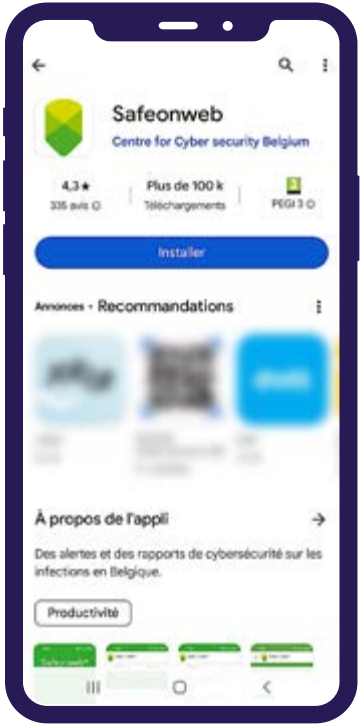
N'effectuez pas de transactions bancaires et ne communiquez pas vos données confidentielles sur des sites sans cadenas ou commençant par « http:// ».

Attention ! Les cybercriminels peuvent eux aussi créer des sites web « https:// » faussement sécurisés. Faites toujours preuve de prudence quand vous devez partager des données importantes, et vérifiez toujours que vous êtes sur le bon site internet.

Utilisez l'application Safeonweb

Si vous désirez vous tenir informé des différentes cybermenaces et des nouvelles arnaques, téléchargez l'application Safeonweb, disponible gratuitement sur l'App Store et Google Play ou surfez sur le site web **www.safeonweb.be**.

Safeonweb.be



Pour vous entraîner à reconnaître un lien menant un site web frauduleux, utilisez leur module sur **https://surfersanssoucis.safeonweb.be/fr/modules/1**

Attention, Safeonweb n'est pas un antivirus mais une plateforme pour vous informer.

L'extension Safeonweb vous aide à évaluer la fiabilité d'un site web en attribuant un niveau de confiance à chaque site: élevé (vert), moyen (orange) ou faible (rouge). Pour installer l'extension sur votre navigateur Internet (uniquement sur ordinateur), consultez https://safeonweb.be/fr/campagne-nationale-de-sensibilisation-la-cybersecurite-2023.

Comment reconnaître une tentative de fraude en ligne ?

Voici quelques éléments qui vous permettront de détecter une tentative de fraude :

> **Un expéditeur suspect :** les fraudeurs 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 ».

Les cybercriminels utilisent des techniques sophistiquées pour copier les logos, les polices de caractère, les images ou encore les signatures dans les e-mails d'entreprises légitimes pour rendre leurs messages plus crédibles. Ils peuvent aussi se faire passer pour ces entreprises par téléphone.

> **L'urgence :** pour vous piéger rapidement, ils créent souvent de fausses urgences comme l'expiration de votre mot de passe ou la perte de l'accès à vos données.

Dans les situations de stress, vous êtes plus susceptible de prendre des décisions moins réfléchies.

> **La curiosité :** les fraudeurs cherchent également à éveiller votre curiosité avec des promesses trop belles pour être vraies, comme un compte d'épargne avec un intérêt à 10% ; un concours pour gagner une voiture de luxe ; le remboursement de votre emprunt immobilier ; un voyage entièrement gratuit…

> **La demande d'informations personnelles :** les fraudeurs en ligne peuvent vous demander, via un lien ou non, des informations personnelles.

Les méthodes de fraude en ligne

L'hameçonnage (*phishing*)

L'hameçonnage, ou *phishing* en anglais, est une fraude au cours de laquelle les fraudeurs tentent de s'emparer des codes bancaires et des données personnelles de leurs victimes. Ils envoient des messages trompeurs encourageant les utilisateurs à divulguer leurs données personnelles sensibles.

Si ces messages frauduleux sont envoyés par SMS, on parle de *smishing*.

Le *phishing* peut aussi se faire par téléphone : les fraudeurs vont inciter les potentielles victimes à divulguer des données personnelles, à signer une transaction avec itsme ou le lecteur de carte ou encore à installer un logiciel.

> Le *phishing* standard

Comment reconnaître un email de *phishing* ?

Ⓐ **L'adresse e-mail ne correspond pas à l'adresse électronique officielle de l'organisation**. En l'examinant de plus près, on remarque qu'il y a une lettre en plus, une lettre en moins, des caractères inhabituels, etc. Les banques et les entreprises n'ont pas de compte Gmail, Yahoo ou Outlook/Hotmail. Un e-mail d'une entreprise se terminant par @gmail, @outlook, @yahoo, @hotmail est donc potentiellement un e-mail frauduleux.

Ⓑ On retrouve parfois **des fautes d'orthographe et de grammaire** dans le texte.

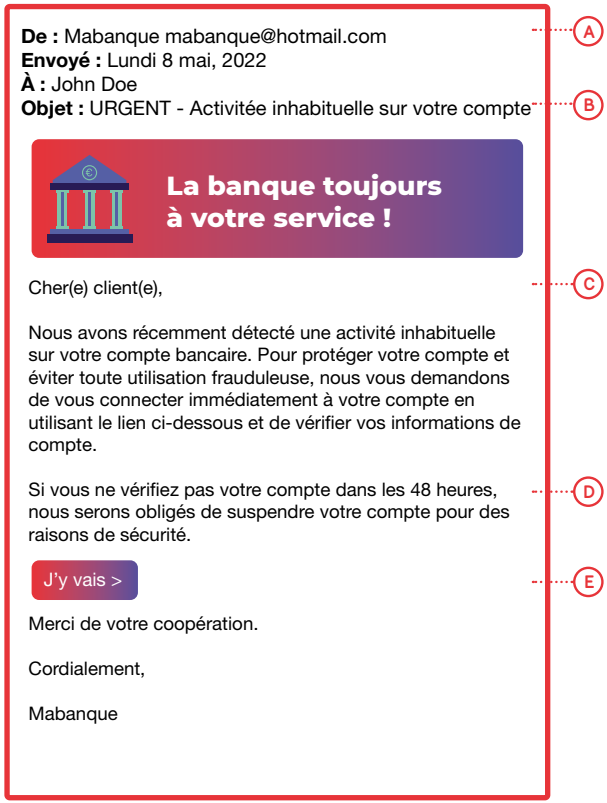
Ⓒ La plupart du temps, **le message ne vous est pas adressé personnellement**.

Ⓓ Les messages de *phishing* vous incitent à passer à l'action en créant **un sentiment d'urgence**.

Ⓔ **Le message vous incitera toujours à cliquer**

sur un lien. Ce lien vous renverra vers une page internet frauduleuse qui vous demandera, soit de donner vos données personnelles et/ou bancaires, soit de télécharger une application ou un logiciel frauduleux. Attention, des escrocs particulièrement ingénieux parviennent parfois à s'adresser à vous personnellement.

Pour être sûr d'être sur la page authentique de votre banque, passez par votre application bancaire ou tapez vous-même l'adresse du site web de votre banque dans votre barre de navigation.



> Le *phishing* à la carte bancaire en ligne

Lors d'une tentative de *phishing* à la carte bancaire, les fraudeurs tentent d'obtenir directement la carte bancaire et les codes bancaires.

Vous recevez un message qui vous indique que vous devez impérativement remplacer votre carte bancaire. Ce message vous incite à cliquer sur un lien. En cliquant dessus, vous arrivez sur une page où l'on vous demande :

1. De compléter **vos données personnelles** et **votre numéro de carte bancaire**.
2. D'introduire **votre code pin actuel** et d'en choisir un nouveau.
3. De renvoyer **votre carte de débit par la poste**. Pour brouiller les pistes, les criminels vont parfois vous demander de découper votre carte en deux en laissant la puce intacte, avant de l'envoyer par la poste.

> Le *phishing* à la carte bancaire à domicile

Le fraudeur peut aussi se faire passer pour un employé de votre banque en se comportant généralement de manière professionnelle afin de gagner votre confiance.

1. **Il vous appelle** pour vous informer que des transactions suspectes ont été effectuées avec votre carte bancaire.
2. Durant l'appel, il prétend que la réception est mauvaise et vous propose de **se rendre directement à votre domicile** afin de résoudre le problème.
3. À votre domicile, le fraudeur vous demande de **vous connecter à la banque en ligne** et se positionne de manière à pouvoir voir vos codes personnels. Ils peuvent aussi vous demander directement vos codes.

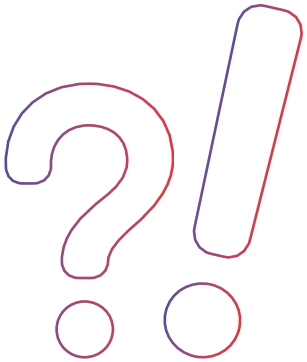
④ Prétextant **des problèmes avec votre carte**, il vous propose ensuite de la reprendre pour que vous en receviez une nouvelle. Il peut aussi vous proposer de détruire votre carte devant vous. Il coupera la carte en deux **sans abîmer la puce**. Avec la puce intacte, il pourra l'utiliser pour vous voler de l'argent.

Conseil en or : si vous devez vous séparer de votre carte bancaire, coupez bien la puce.

Les employés de banque ne vous demanderont jamais votre code pin ou la réponse donnée sur votre lecteur de carte. Ils ne viendront jamais à votre domicile ni pour détruire ou récupérer votre carte bancaire, ni pour résoudre des problèmes de paiement.

Que se passe-t-il lorsqu'on clique sur un lien frauduleux ?

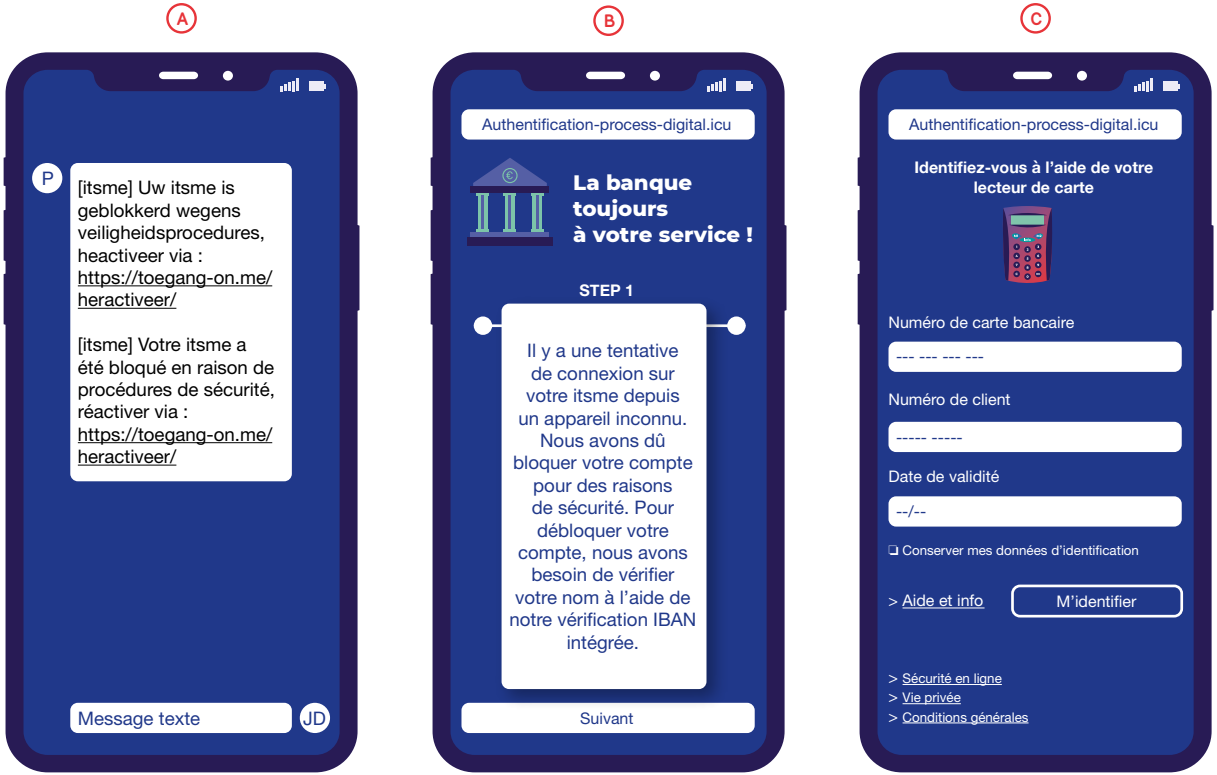
Si vous cliquez sur un lien frauduleux, vous arrivez sur un site Internet qui imite souvent très bien le site internet de votre banque. L'objectif ici est de récupérer vos données personnelles et vos codes bancaires.



Ⓐ Voici un exemple de *smishing* (*phishing* par SMS) au nom d'itsme.

Ⓑ En cliquant sur le lien, vous arrivez sur une page où on vous explique qu'il y a des tentatives pour se connecter à votre compte itsme depuis un appareil inconnu. Ensuite, on vous demande de choisir votre banque et vous êtes dirigé sur une fausse page de connexion à votre banque.

Ⓒ On vous invite à encoder vos informations bancaires sur une page qui ressemble beaucoup à l'environnement de votre banque : même logo, même couleur, même écriture.


A
P
[itsme] Uw itsme is geblokkerd wegens veiligheidsprocedures, heactiveer via : https://toegang-on.me/heractiveer/
[itsme] Votre itsme a été bloqué en raison de procédures de sécurité, réactiver via : https://toegang-on.me/heractiveer/
Message texte
JD
B
Authentification-process-digital.icu
La banque toujours à votre service !
STEP 1
Il y a une tentative de connexion sur votre itsme depuis un appareil inconnu. Nous avons dû bloquer votre compte pour des raisons de sécurité. Pour débloquer votre compte, nous avons besoin de vérifier votre nom à l'aide de notre vérification IBAN intégrée.
Suivant
C
Authentification-process-digital.icu
Identifiez-vous à l'aide de votre lecteur de carte
Numéro de carte bancaire
--- --- --- ---
Numéro de client
----- -----
Date de validité
--/--
❑ Conserver mes données d'identification
> Aide et info
M'identifier
> Sécurité en ligne
> Vie privée
> Conditions générales

Fraudes où la victime est invitée à faire un virement elle-même

On observe depuis 2021 une évolution vers de nouvelles formes de fraude dans lesquelles les victimes sont poussées à transférer elles-mêmes de l'argent.

> La fraude aux comptes à sécurité renforcée

Ici, le cybercriminel vous approche généralement en deux ou trois étapes :

- **Il vous envoie d'abord un message** vous demandant vos codes bancaires afin de se frayer un accès à votre compte.
- **Ensuite, il vous appelle en se faisant passer pour un employé de votre banque.** Parfois, il commence directement par cette étape.
- **Il mentionne que votre compte est en danger.**
- **Enfin, il vous invite à transférer votre argent** vers un nouveau compte réputé hautement sécurisé.

Attention ! Tous les comptes en banque ont un niveau de sécurité élevé. Ce type de compte « à sécurité renforcée » n'existe donc pas !

N'oubliez pas que votre banque ne vous demandera jamais par téléphone, e-mail, SMS ou via les réseaux sociaux de transférer votre argent vers un autre compte.

> La fraude à l'amitié

La fraude à l'amitié, également connue sous le nom de fraude amoureuse ou arnaque à l'affection, est une technique utilisée par les fraudeurs pour gagner la confiance des victimes en se faisant passer pour des amis ou des partenaires romantiques en ligne.

1. Les fraudeurs créent de faux profils sur les sites de rencontre ou les réseaux sociaux et se font passer pour des personnes de confiance. Pour ce faire, ils utilisent des photos et des informations personnelles volées ou falsifiées pour se faire passer pour des personnes réelles.
2. Ils établissent ensuite une relation avec leur victime en communiquant régulièrement avec elle par e-mail, téléphone ou chat.
3. Au fil du temps, les fraudeurs utilisent cette relation pour obtenir de l'argent ou des informations personnelles de la victime. Ils peuvent demander de l'argent pour des dépenses imprévues, comme des factures médicales ou des billets d'avion, ou demander des informations sensibles telles que des numéros de carte de crédit ou de sécurité sociale.

Faites preuve de prudence et de vigilance lors de la création de relations en ligne. Si vous êtes contacté par une personne que vous ne connaissez pas ou si quelque chose vous semble suspect, n'hésitez pas à prendre du recul et à faire des recherches pour vous assurer que la personne est bien réelle et digne de confiance. S'il vous reste le moindre doute, ne transférez pas d'argent !

> La fraude à la demande d'aide

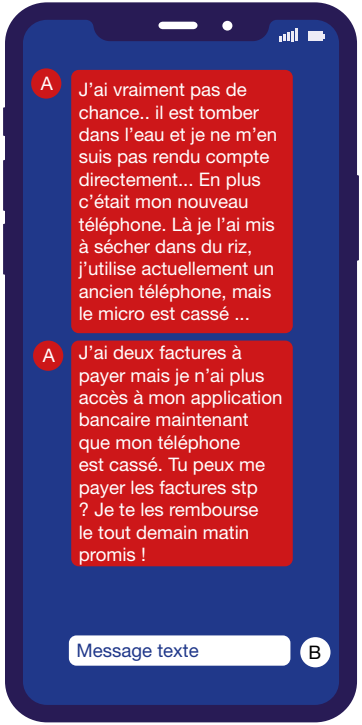
Lorsqu'un cybercriminel utilise cette méthode :

1. Il vous contacte par e-mail, SMS ou via les réseaux sociaux
2. Il se fait passer pour l'un de vos proches
3. Enfin, il vous explique qu'il est dans une situation financière urgente et vous demande de lui faire un virement directement sur un numéro de compte.

Le fraudeur peut également écrire à vos proches en votre nom.

Conseil en or : appelez vous-même l'expéditeur du message pour vérifier son identité. Posez-lui des questions personnelles dont les réponses ne figurent pas dans de précédents e-mails, chats ou sur les réseaux sociaux.


A
Coucou mamie c'est mon nouveau numéro, j'ai un soucis avec mon gsm. tu peux enregistrer ce numéro
OK, c'est fait !
B
Ah zut !
B
A
Ca me dépanne quand même, au moins je peux t'écrire. Comment vas-tu ?
Je vais très bien mon chéri Et toi, à part ton téléphone cassé, ça va ?
B
A
Pas trop non. Comme si ça ne suffisait pas j'ai un autre problème là...
Est-ce que je peux t'aider ?
B


A
J'ai vraiment pas de chance.. il est tomber dans l'eau et je ne m'en suis pas rendu compte directement... En plus c'était mon nouveau téléphone. Là je l'ai mis à sécher dans du riz, j'utilise actuellement un ancien téléphone, mais le micro est cassé ...
A
J'ai deux factures à payer mais je n'ai plus accès à mon application bancaire maintenant que mon téléphone est cassé. Tu peux me payer les factures stp ? Je te les rembourse le tout demain matin promis !
Message texte
B

> La fraude à l'investissement

Dans le cas de la fraude à l'investissement, le fraudeur essaie de soutirer de l'argent aux victimes en leur proposant un investissement avec un rendement très intéressant. On découvre par la suite que l'investissement proposé n'existe pas ou qu'il rapporte bien moins que prévu. Avez-vous été contacté par un inconnu vous proposant d'investir ? Redoublez de vigilance si vous observez les situations suivantes :

- Vous êtes contacté de manière non sollicitée par téléphone ou par e-mail sans savoir comment le fournisseur a obtenu vos données.
- Le fournisseur ne s'identifie pas et refuse de donner son adresse physique «pour des raisons de confidentialité».
- Il vous promet des rendements ou des bénéfices exceptionnellement élevés.
- Vous ne recevez pas d'autres détails sur l'investissement, même si vous en demandez explicitement.
- Le fournisseur est situé dans un autre pays.
- On vous demande de transférer l'argent sur un compte en banque hors Belgique (le numéro de compte ne commence pas par «BE»).
- Vous êtes mis sous pression pour prendre une décision rapide.

Si vous avez été contacté par un inconnu vous proposant d'investir :

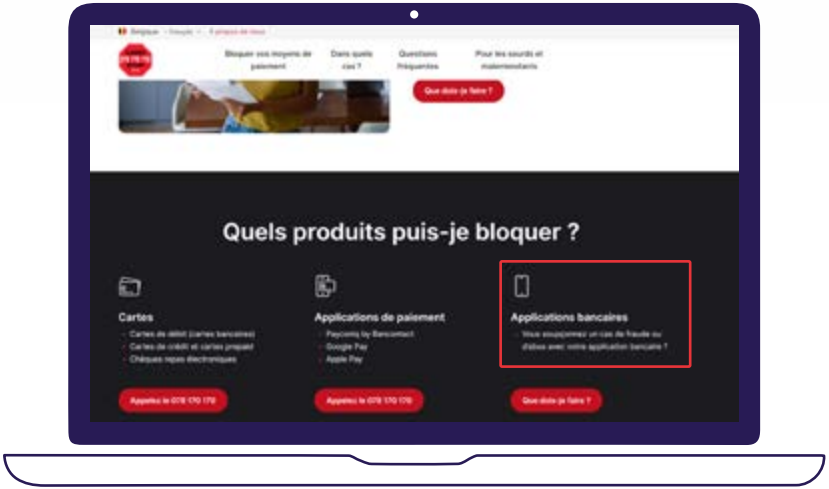
1. Vérifiez toujours l'identité du fournisseur : soyez critique avec les informations que vous trouvez sur Internet. Pas d'informations claires et fiables ? N'acceptez pas l'offre.
2. Ne partagez jamais vos données personnelles : les fraudeurs demandent souvent une copie de votre carte d'identité, une photo, un numéro de carte bancaire ou de carte de crédit, etc. Ne répondez pas !
3. Exigez des informations claires et compréhensibles et informez-vous soigneusement sur l'offre. Si vous ne la comprenez pas, ignorez-la.
4. Méfiez-vous de la promesse d'un bénéfice excessif : si un rendement semble trop beau pour être vrai, c'est généralement parce qu'il n'est pas vrai. Le bénéfice n'est jamais garanti.

Qui contacter en cas de fraude ?

Si vous avez malgré tout été victime d'une fraude, vous devez :

1. Contactez le plus vite possible votre banque pour qu'elle puisse bloquer l'accès à votre compte bancaire. Chaque banque a un service fraude disponible 24 heures sur 24, 7 jours sur 7.

Sur le site de votre banque et de Card Stop (illustré ci-dessous), vous trouverez une page avec les coordonnées de votre banque que vous pouvez joindre si vous avez été victime de fraude ou de *phishing*.



② Contactez également Card Stop pour bloquer votre carte au 078 170 170. Ce numéro est aussi accessible depuis l'étranger via le +32 78 170 170.

③ Déposez une plainte auprès de la police.

Police

Exercices : de quel type de fraude s'agit-il ?

Trouvez tous les indices !

Exercice 1

e-mail

Objet : URGENT - Mise à jour de vos informations de carte bancaire

Cher(e) client(e),

Nous vous écrivons pour vous informer qu'il est temps de mettre à jour les informations de votre carte bancaire. Nous avons récemment mis en place des mesures de sécurité supplémentaires pour protéger vos transactions et nous avons besoin de votre coopération pour les mettre en place.

Veuillez compléter vos données personnelles et fournir votre numéro de carte bancaire complet. De plus, nous vous demandons de bien vouloir introduire votre code PIN actuel et d'en choisir un nouveau pour votre sécurité.

Nom :

Prénom :

Numéro de téléphone :

Numéro de carte bancaire :

Code PIN :

Pour des raisons de sécurité, nous souhaitons également vous informer que nous avons besoin que vous renvoyiez votre carte de débit par la poste à l'adresse suivante : Rue de la Fraude, 12 – 23145 Syber, Belgique.

Nous prenons très au sérieux la sécurité de nos clients, c'est pourquoi nous demandons votre coopération pour mettre à jour vos informations de carte bancaire.

Nous vous remercions de votre coopération.

Cordialement,

L'équipe de MaBanque

Exercice 2

e-mail

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

Exercice 3

sms

BePost : 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/7lgWRa

Exercice 4

Message Whatsapp

Mon amour je le suis faits agressés par des bandits, après faire le retrait d'argent pour donner au Docteur ils m'ont tout pris mon amour l'argent que j'ai retiré je n'ai plus rien chérie je ne sais plus comment faire pour payer le dernière montant que le docteur m'a demandé pour l'opération de ma m !re ils m'ont aussi pris ma carte bancaire je ne sais plus comment faire mon amour tous mes papiers, la seule choses est que j'avais laissé mon téléphone ici et je l'avais oublié et aussi je suis un peu touché car je n'ai pas voulu me laisser faitre en essayant de résister mais il mon tabasser comme un chien le coursier de ma mère a reçu une balle dans le pied j'ai mal partout mon Amour .

G Notes

Cette brochure a été réalisée par **Paradigm** en collaboration avec la **Fédération belge du secteur financier (Febelfin)** dans le cadre du **Plan d'Appropriation Numérique 2021 – 2024.**

Contact : inclusion@paradigm.brussels

RÉGION DE BRUXELLES-CAPITALE

paradigm .brussels

febelfin

ER : Paradigm - Nicolas Locoge - Avenue des Arts, 21 - 1000 Bruxelles. Ne pas jeter sur la voie publique.