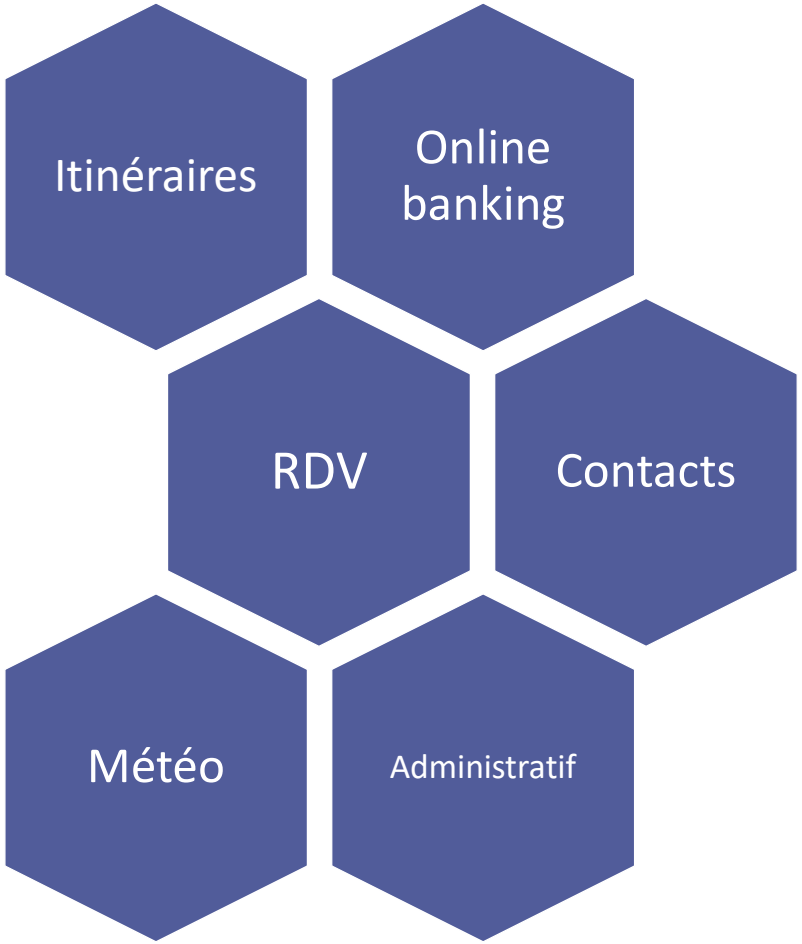
Les bons réflexes en matière de cybersécurité

Cathy Grimmeau - CCB

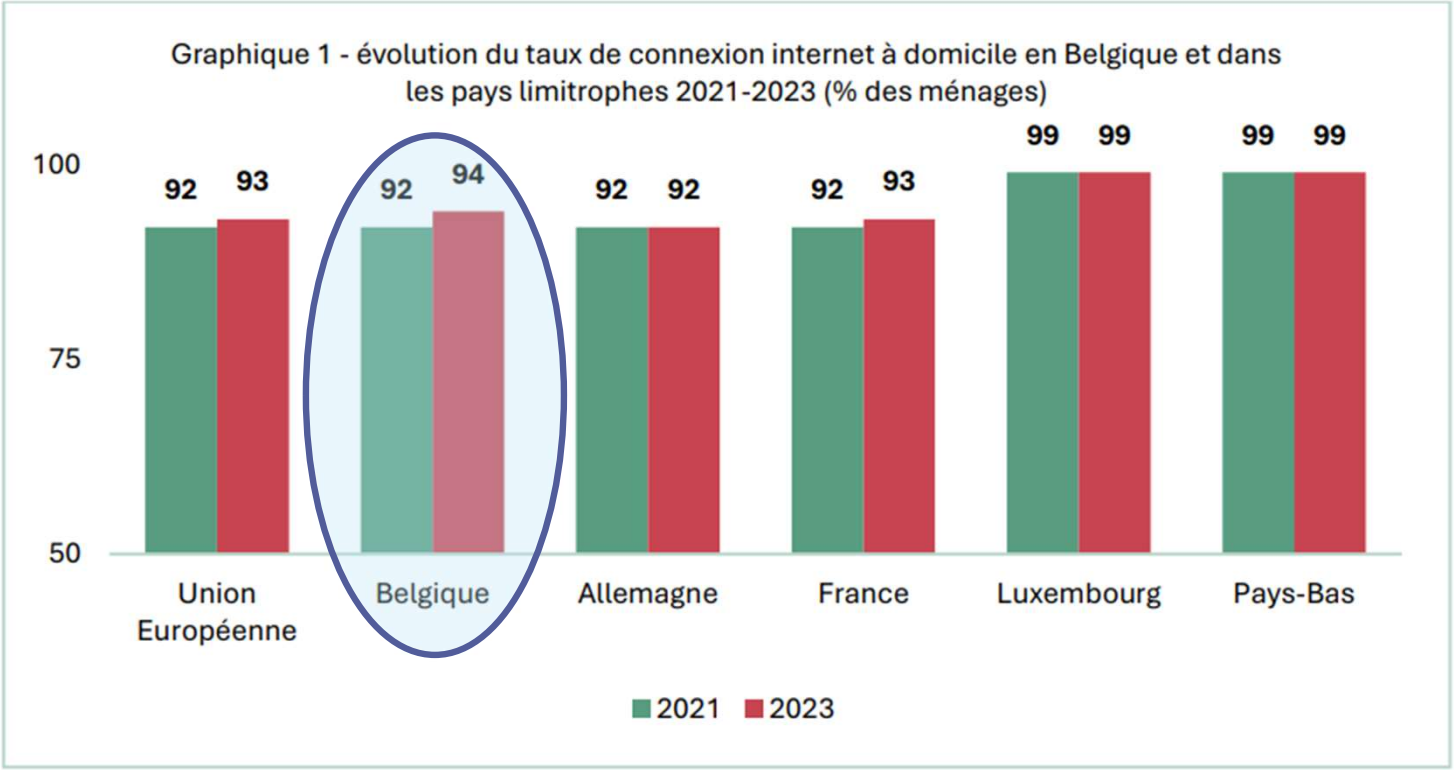
Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Qui peut encore passer à côté d'Internet ?

CENTRE FOR CYBERSECURITY BELGIUM



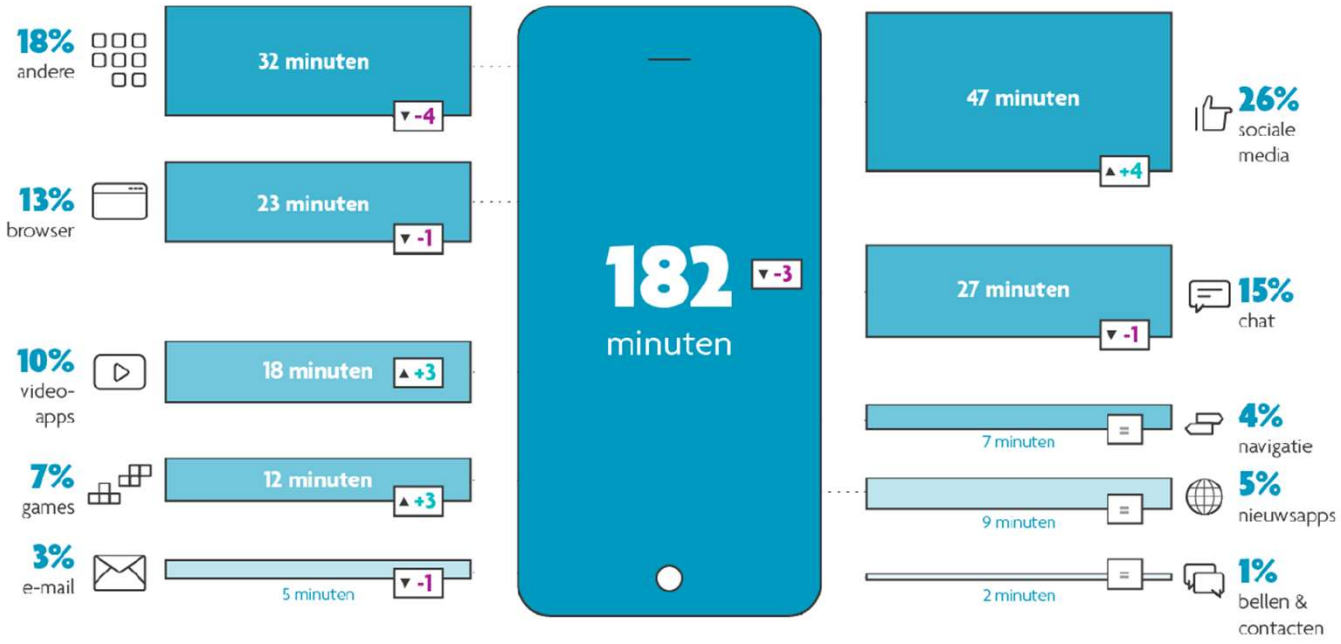
Tout le monde est sur Internet



Source : calculs IACCHOS, UCLouvain, d'après les enquêtes Statbel 2021 et 2023.

Schermtijd

Wat doet de Vlaming zoal op zijn smartphonescherm?



Digimètre Imec, 2023

Les cybercriminels se frayent également un chemin

- **Phishing, smishing**
  - Escroqueries par mails ou SMS suspects : vous donnez vos coordonnées bancaires ou transférez une somme sur le compte d'escrocs.
- **Piratage**
  - Les pirates ont accès à vos comptes (Facebook, mail, etc...), ils envoient des messages en votre nom, font des commandes en votre nom, etc....
- **Escroquerie aux investissements en crypto-monnaie**
  - Les escrocs vous encouragent à investir dans les crypto-monnaies par l'intermédiaire de fausses plateformes de trading.
- **Sextorsion**
  - L'escroc prétend posséder des images sexuellement explicites de vous. Il s'agit d'un bluff. Il menace de partager les images si vous ne payez pas.
- **Escroquerie Microsoft**
  - Vous recevez un appel d'une personne qui prétend être un employé de Microsoft, Apple ou Proximus. La personne prétend qu'il y a un problème avec l'appareil et veut vous aider, si vous payez.
- **Et de nombreuses autres formes de fraude en ligne se développent**

CENTRE FOR CYBERSECURITY BELGIUM

L’authentification à deux facteurs

CENTRE FOR CYBERSECURITY BELGIUM

5 conseils pour se protéger en ligne

5 conseils pour se protéger en ligne

CENTRE FOR CYBERSECURITY BELGIUM

- Apprendre à reconnaître le phishing
- Télécharger uniquement à partir de stores reconnus
- Faire des sauvegardes
- Effectuer les mises à jour
- Utiliser un antivirus

CENTRE FOR CYBERSECURITY BELGIUM

Le sixième conseil = le meilleur conseil

Utilisez l’authentification à deux facteurs partout où vous le pouvez !

CENTRE FOR CYBERSECURITY BELGIUM

Quelques chiffres

- **71 %** des personnes interrogées connaissent le terme « authentification à deux facteurs»
- **55 %** savent également ce qu'il signifie exactement
- En Flandre et à Bruxelles, le terme et le concept sont plus familiers qu'en Wallonie
  - Flandre : 77% connaissent le terme
  - Bruxelles : 70% connaissent le terme
  - Wallonie : 60% connaissent le terme
- Effet d'âge :
  - 18-24 ans : 72% connaissent le terme
  - 25-34ans : 75% connaissent le terme
  - 35-44ans : 85% connaissent le terme
  - 45-54ans : 73% connaissent le terme
  - 55-64ans : 70% connaissent le terme
  - **65+ : 55% connaissent le terme**

Enquête Omnibus Safeonweb – juillet 2024 – échantillon 1000 Belges

Quelques chiffres

- **64% de l'échantillon total est conscient de l'utilité de l'authentification à deux facteurs**

  La prise de conscience est plus élevée parmi ceux qui connaissent le terme '2FA'

- **Utiliser l'authentification à deux facteurs:**
  - La moitié des utilisateurs de l'échantillon global déclarent utiliser l'authentification à deux facteurs pour au moins un compte :
    - **57%** sur les sites web où les données bancaires sont enregistrées (par exemple, achats en ligne, réservation de voyages, achat de tickets,...)
    - **51%** sur les comptes professionnels
    - **52%** sur les comptes de messagerie privée
    - **47%** sur les comptes de médias sociaux
    - **35%** sur les comptes de jeux
  - **En Wallonie, ce chiffre est nettement inférieur**

Quelques chiffres

- La 2FA permet de réduire de 99 % le piratage de comptes :
  - Les mots de passe volés par piratage sont inutiles avec l'utilisation de la 2FA.
  - Les logiciels malveillants et les virus ne peuvent plus avoir d'impact sur la sécurité des comptes utilisant la 2FA.
  - Les comptes paramétrés avec la 2FA ont un risque de piratage considérablement réduit.

Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits; 12/2023; https://www.enterpriseappstoday.com/stats/two-factor-authentication-statistics.html#:~:text=According%20to%20TechCrunch%2C%20Facebook%202FA,more%20than%201.5%20million%20accounts.&text=95%25%20of%20companies%20that%20used,benefits%20of%20software%2Dbased%20authentication

L’authentification à deux facteurs ou …

CENTRE FOR CYBERSECURITY BELGIUM

2FA

MFA

La vérification en deux étapes

La validation en deux étapes

Authentification quoi ? Qu'est-ce que la 2FA ?

Il s'agit d'une mesure de sécurité visant à empêcher les pirates ou les escrocs d'accéder à vos comptes en utilisant deux formes d'authentification différentes :

- Ce que vous connaissez : mot de passe
- Ce vous avez : smartphone
  - Code reçu par SMS,
  - Application (Itsme, Authenticator App, etc.),
- Ce qui vous rend unique: empreinte digitale, reconnaissance faciale, ...

Image : Kaspersky

Et la MFA alors?

Lorsqu’on utilise plus que 2 facteurs de protection on parle de Multi Factor Authentication ou MFA

Si seulement ils avaient utilisé l'authentification à 2 facteurs

CENTRE FOR CYBERSECURITY BELGIUM

MERCREDI 26 JUIN 2024 SUDINFO 7

FLOREFFE

LES PAGES DU « BAROMÈTRE » HACKÉES : LE PIRATE DEMANDE 250€ POUR LES RÉSERVATIONS

Le restaurant « Le Baromètre » à Floreffe a rouvert il y a quelques semaines après une courte pause. Mais le patron a des soucis avec les réservations. Il demande aux clients de lui sonner directement pour réserver afin d'éviter les arnaques en ligne.

Les lieux existent depuis sept ans. © F.B.

SHANTI DUPARQUE

La brasserie « Le Baromètre », situé rue Camille Giroul à Floreffe, a rouvert après une interruption hivernale.

Le chef, Christophe Delahaye, propose à nouveau ses plats préparés minute dans sa cuisine ouverte. Mais depuis deux mois, il galère un peu pour ses réservations. Pourtant, les clients sont toujours nombreux à vouloir venir chez lui.

Le souci se pose ailleurs : « Depuis presque deux mois, mon compte Facebook a été hacké par une personne malintentionnée qui répond à ma place aux demandes de réservation », commence le chef.

BESOIN D'UN PRO

« Au début, ce hacker demandait même aux clients de verser un acompte de 250 euros pour confirmer leur réservation. Heureusement, il n'avait pas laissé de numéro de compte donc personne ne s'est fait avoir »

Le chef tente de joindre quelqu'un chez Facebook pour régler le souci. « En fait, mon compte privé a été piraté et donc mes cinq pages commerces liés à celui-ci, comme celle du restaurant et de la chambre d'hôtes, sont aussi inaccessibles ».

Il précise à ses clients que pour réserver, la seule possibilité est de téléphoner au 081 45 16 91. « Et évidemment aucun acompte ne vous sera demandé ».

Le chef, un peu désemparé, en profite pour lancer un appel : « Si vous avez des solutions ou l'expérience pour récupérer un compte piraté, vous pouvez me contacter sur la ligne fixe, bien évidemment », précise le restaurateur. ■

Piratage chez Ticketmaster : attention si vous avez utilisé cette plateforme, voici les mesures à prendre contre le vol de votre argent

100 millions de mots de passe volés et publiés en ligne. Voici comment vérifier si les vôtres en font partie

6 LA MEUSE MERCREDI 21 FÉVRIER 2024

LIÈGE

La messagerie de Willy Demeyer piratée

On a beau être bourgmestre d'une des plus grandes villes du pays, on n'est pas à l'abri d'une usurpation d'identité. Willy Demeyer, le bourgmestre de Liège, vient d'en faire les frais.


Willy Demeyer est victime d'une usurpation d'identité. © MT

Des mails d'amis « coincés à l'étranger », privés de tous leurs papiers d'identité et de leurs cartes bancaires, ou de services, publics ou privés, qui réclament le montant d'une facture impayée, tout le monde en a déjà reçu. Et chacun sait donc que verser de l'argent pour les aider à se tirer d'affaires est tout sauf une bonne idée. Mais quand ce mail émane du bourgmestre de Liège et arrive sur la messagerie d'un Liégeois, ça pourrait prêter à confusion. Sauf que ce n'est évidemment jamais le bourgmestre qui se charge des rappels des paiements…

C'est pourtant ce qui risque d'arriver dans les prochains jours. Mais sur le sujet, M. Demeyer est clair : « Si on vous demande de l'argent à mon nom, merci de ne rien me verser. Mon compte a été piraté. »

Selon les premiers éléments, il semblerait qu'un escroc ait créé une adresse mail au nom du bourgmestre. Et s'en serve donc maintenant pour réclamer des versements. Une usurpation d'identité donc, conte laquelle le bourgmestre lui-même a voulu mettre en garde. ■

G.W.

Pourquoi protéger vos comptes en ligne?

CENTRE FOR CYBERSECURITY BELGIUM

Les cybercriminels qui ont accès à vos comptes :

- Peuvent vous faire vivre un **cauchemar financier**
  - accès à vos comptes de paiement en ligne
  - achats en votre nom
  - fraude en votre nom
- Peuvent prendre le contrôle de votre **identité en ligne**
  - Atteinte à la réputation
  - Escroquerie de vos amis et de votre famille en votre nom
  - Accès aux informations personnelles

Comment savoir si mon compte a été piraté ?

CENTRE FOR CYBERSECURITY BELGIUM

- Vous recevez un mail qui indique une connexion avec un nouvel appareil
- Vous constatez des activités suspectes: ex: derniers films vus sur Netflix
- Vos amis vous disent avoir reçu un mail étrange de votre part
- Vous constatez un paiement frauduleux sur votre compte
- Des publications étranges apparaissent sur vos réseaux sociaux

Mon compte est piraté, que faire ?

CENTRE FOR CYBERSECURITY BELGIUM

- Comment retrouver le contrôle de votre compte ?
  - Vous avez encore accès à votre compte ? Modifiez alors immédiatement le mot de passe de ce compte et de tous vos autres comptes.
  - Vous n'avez plus accès à votre compte ? Utilisez les options de restauration pour retrouver l'accès et modifiez ensuite tous vos mots de passe.
- Que faire de plus ?
  - Scannez votre ordinateur à la recherche de virus.
  - Si vos données bancaires ont été volées, avertissez votre banque et contactez Card Stop au 078 170 170 si vous constatez des transactions suspectes.
- Si des données professionnelles ont été volées, avertissez au plus vite votre employeur.
- Activez la 2FA

Les mots de passe sont dépassés

CENTRE FOR CYBERSECURITY BELGIUM

- Les mots de passe sont frustrants
- Nous continuons à utiliser des mots de passe faibles
- Mais même les mots de passe forts ne sont pas sûrs...

50 Most Commons Passwords 2024

CENTRE FOR CYBERSECURITY BELGIUM

https://www.rd.com/article/passwords-hackers-guess-first/

CENTRE FOR CYBERSECURITY BELGIUM

Même un mot de passe fort n'est pas sûr

CENTRE FOR CYBERSECURITY BELGIUM

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Comment les pirates informatiques volent-ils votre mot de passe ?

CENTRE FOR CYBERSECURITY BELGIUM

- Ils volent votre mot de passe par le biais du **phishing** ou de faux messages.
- Une **fuite de données** dans un service en ligne d'une entreprise pourrait laisser votre mot de passe à la portée de tous sur internet.
- Avec les **virus** qui volent les mots de passe

Nous facilitons la tâche des pirates informatiques !

CENTRE FOR CYBERSECURITY BELGIUM

- Nous écrivons les mots de passe sur des post-it
- Nous révélons les mots de passe au téléphone
- Nous donnons un mot de passe lors d'un faux concours en ligne

Comment éviter cela ?

CENTRE FOR CYBERSECURITY BELGIUM

- Utiliser l'authentification à deux facteurs lorsque c'est possible
  - Commencez par votre compte mail
  - Activez-la sur les sites web où vous laissez vos coordonnées bancaires : sites d'achats en ligne, sites de réservation de location de vacances, site de réservation de tickets, site de revente, …
  - Protégez vos médias sociaux avec la 2FA

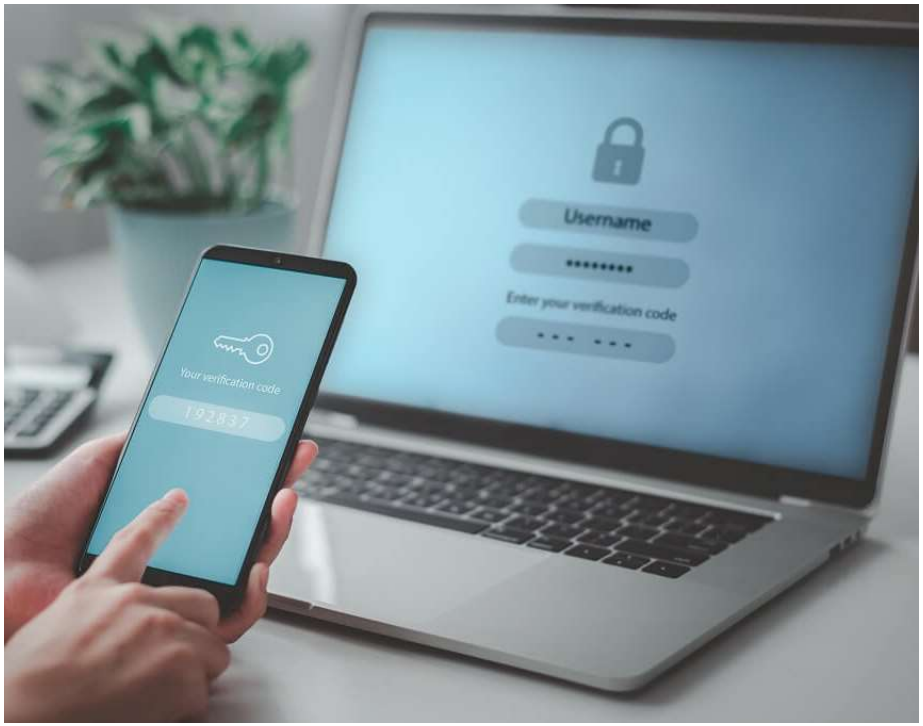
Bref, prenez l'habitude de l'utiliser partout où elle est disponible

Comment activer la 2FA ?

CENTRE FOR CYBERSECURITY BELGIUM

L'activation de la 2FA varie d'une plateforme à l'autre, mais les étapes sont généralement assez similaires :

- Accédez aux paramètres de sécurité du compte que vous souhaitez sécuriser.
- Recherchez l'option permettant d'activer la 2FA et sélectionnez-la.
- Choisissez le deuxième facteur que vous souhaitez utiliser (par exemple, SMS, application d'authentification, etc.).
- Suivez les instructions à l'écran pour configurer le deuxième facteur.
- Testez si tout est configuré correctement en vous déconnectant et en vous connectant à nouveau avec le deuxième facteur.



Quel est le meilleur deuxième facteur?

CENTRE FOR CYBERSECURITY BELGIUM

- Le deuxième facteur que vous utilisez n'a pas d'importance*. Deux facteurs de sécurité valent toujours mieux qu'un seul.
- Utilisez deux types de facteurs différents, et non pas, par exemple, deux fois quelque chose que vous connaissez.
- ** Un code envoyé par SMS est facile à obtenir et ce système est généralement bien connu. C'est peut-être la solution la plus accessible, mais... les escrocs essaient de l'obtenir en échangeant la carte SIM. Si l'escroc parvient à s'emparer de votre téléphone et qu'il n'est pas verrouillé ou qu'il affiche les messages même lorsqu'il est verrouillé, il peut alors utiliser le code...*

SMS ou application d'autentification?

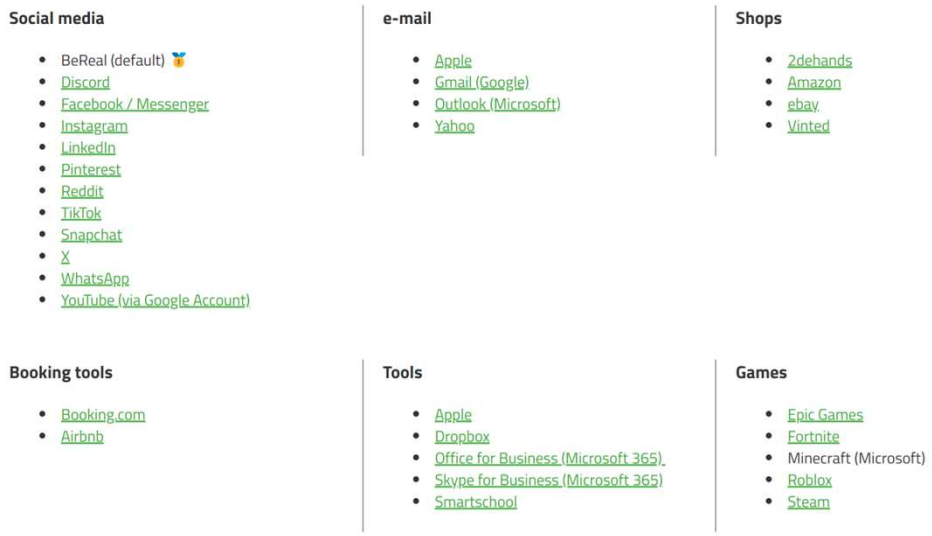
CENTRE FOR CYBERSECURITY BELGIUM

- Application Authenticator : vous téléchargez une application via App Store ou Google Play (par exemple Google Authenticator ou Microsoft Authenticator). Via un code QR, vous ajoutez le compte à votre application. Chaque fois que vous vous connectez, l'application génère un code à usage unique que vous insérez à l'endroit indiqué.
- SMS : vous entrez votre numéro de téléphone et vous recevez un SMS contenant un code que vous devez saisir à l'endroit indiqué.
- C'est un choix libre (en fonction de la maturité du public cible)
- Important: ne jamais partager les codes!!!

Vous avez des doutes ?

CENTRE FOR CYBERSECURITY BELGIUM

- Voir comment utiliser la 2FA sur les comptes les plus couramment utilisés sur Safeonweb
- https://safeonweb.be/en/two-factor-authentication-it-difficult-use



Social media

- BeReal (default)
- Discord
- Facebook / Messenger
- Instagram
- LinkedIn
- Pinterest
- Reddit
- TikTok
- Snapchat
- X
- WhatsApp
- YouTube (via Google Account)

e-mail

- Apple
- Gmail (Google)
- Outlook (Microsoft)
- Yahoo

Shops

- 2dehands
- Amazon
- ebay
- Vinted

Booking tools

- Booking.com
- Airbnb

Tools

- Apple
- Dropbox
- Office for Business (Microsoft 365)
- Skype for Business (Microsoft 365)
- Smartschool

Games

- Epic Games
- Fortnite
- Minecraft (Microsoft)
- Roblox
- Steam

Vous avez des doutes?

CENTRE FOR CYBERSECURITY BELGIUM

- Demandez de l'aide à quelqu'un à qui vous faites confiance: un membre de la famille, des amis ou les Espaces Publics Numériques (EPN).

Excuses stupides pour ne pas utiliser la 2FA

CENTRE FOR CYBERSECURITY BELGIUM

- Je perds trop de temps avec ça !
  - Quelques secondes seulement. Négligeable par rapport au temps que l'on perd en cas de piratage.
- Et si je perds mon téléphone ?
  - Vous pouvez toujours saisir une adresse électronique de récupération, ou récupérer et enregistrer des codes.

Une mauvaise idée

CENTRE FOR CYBERSECURITY BELGIUM

- Si j'utilise un deuxième facteur, puis-je choisir un mot de passe faible ?
  - Ce n'est pas une bonne idée. L'idée est de choisir deux méthodes sûres. Un mot de passe faible n'est jamais une bonne idée.

Si l’authentification à deux facteurs (2FA) n’est pas disponible pour un service particulier

CENTRE FOR CYBERSECURITY BELGIUM

- Assurez-vous que votre mot de passe est complexe et différent des mots de passe utilisés pour d’autres comptes.
- Vérifiez régulièrement votre compte pour détecter toute activité inhabituelle ou tout accès non autorisé.
- Mettez en place des notifications pour les activités du compte, telles que les connexions ou les modifications de paramètres.
- Utilisez les autres fonctions de sécurité fournies par le service, telles que les questions de sécurité ou les options de récupération de compte.
- Envisagez de passer à un fournisseur de services qui offre des fonctions de sécurité robustes, y compris la 2FA.

Est-il impossible de hacker la 2FA?

CENTRE FOR CYBERSECURITY BELGIUM

- Les escrocs peuvent également essayer d'obtenir votre deuxième facteur de protection :
  - en vous appelant et en utilisant une excuse pour vous convaincre de partager votre code ou d'utiliser Itsme (pour une authentification que l'escroc a lui-même demandée !)
  - En vous envoyant un message de phishing
  - En volant votre téléphone et en utilisant les codes qui s'y trouvent
- Ne partagez donc jamais vos codes avec quelqu'un qui vous les demande !

CENTRE FOR CYBERSECURITY BELGIUM

Campagne 2024

Les craintes des citoyens

Qu'est-ce que nous voulons atteindre en fin de compte ?

Aujourd'hui, les gens ont peur de faire des erreurs lors de l'utilisation de la 2FA.

Nous voulons que les gens se sentent mal à l'aise s'**ils n'utilisent pas la 2FA.**

Nous voulons que tous les Belges utilisent la 2FA

CENTRE FOR CYBERSECURITY BELGIUM

- Nous voyons grand, mais commençons à petite échelle.
- A Herstappe ! Herstappe ?

CENTRE FOR CYBERSECURITY BELGIUM

Matériel disponible

Affiches


Suivez l'exemple de Herstappe : empêchez les cybercriminels d'entrer
Protégez vos comptes en ligne avec l'authentification à deux facteurs. Surfez rapidement sur safeonweb.be
febelfin
.be
Safeonweb


Bruxelles sera-t-elle aussi sûre que Herstappe ?
Suivez l'exemple de Herstappe :
activez l'authentification à deux facteurs et empêchez les cybercriminels d'entrer. Surfez rapidement sur safeonweb.be safeonweb.be
febelfin
.be
Safeonweb

Infographique

Brochure

Comment activer l'authentification à deux facteurs?

L'activation de la 2FA varie d'une plateforme à l'autre, mais les étapes sont généralement assez similaires :

1. **Accédez aux paramètres de sécurité** du compte que vous souhaitez sécuriser.
2. **Recherchez** l'option permettant d'activer la **2FA** et sélectionnez-la.
3. **Choisissez le deuxième facteur** que vous souhaitez utiliser (par exemple, SMS, application d'authentification, etc.).
4. **Suivez les instructions** à l'écran pour configurer le deuxième facteur.
5. **Testez** si tout est configuré correctement en vous déconnectant et en vous connectant à nouveau avec le deuxième facteur.

Safeonweb.be

Par où commencer ?

- Commencez par votre compte mail
- Activez-la sur les sites web où vous laissez vos coordonnées bancaires : sites d'achats en ligne, sites de réservation de locations de vacances, site de réservation de tickets, site de revente, ...
- Protégez vos médias sociaux avec la 2FA

Bref, prenez l'habitude de l'utiliser partout où elle est disponible.

Besoin d'aide ?

N'hésitez pas à demander de l'aide à votre famille ou des amis. Les collaborateurs des Espaces publics numériques (EPN) en Wallonie et Bruxelles sont également à votre disposition.

Plus d'infos ?

Surfez sur **safeonweb.be**

Suivez l'exemple de Herstappe : empêchez les cybercriminels d'entrer

Protégez vos comptes en ligne avec l'authentification à deux facteurs.
Surfez rapidement sur **safeonweb.be**

febelfin .be

Safeonweb.be


QUIZ!

CENTRE FOR CYBERSECURITY BELGIUM

Les fraudes à l'investissement

Fraude à l'investissement

CENTRE FOR CYBERSECURITY BELGIUM

Les escrocs à l'investissement en ligne soutirent en moyenne 20.000 euros à leurs victimes

Arnaque en ligne : la monnaie virtuelle qui crée un trou réel dans vos finances

Arnaque aux cryptomonnaies : ai-je une chance de récupérer mon argent ?

40% des jeunes investisseurs se sont déjà fait arnaquer

La fraude à l'investissement fait des ravages en Belgique

l'avenir

Boutique

ma région | Sports | Nos séries | Santé | Lifestyle | Conseils jardin | Culture

Actu > Belgique

Les chiffres de la fraude en Belgique: diminution des cas de phishing, les fraudes à l'investissement augmentent fortement (infographies)

En 2024, les plaintes pour hameçonnage ont connu une baisse importante. Les cas de phishing, soit le vol de données personnelles sur internet, ont diminué de 26% par rapport à 2023. Malgré tout, les autres types de fraude, notamment à l'investissement, augmentent fortement.

Belga

Publié le 01-04-2025 à 15h23

Enregistrer

L'Echo

Actualité | Invest

Aion Bank d'amende p intérêts sur

ACTU | ECO

MON ARGENT

2024, année record pour les fraudes à l'investissement en Belgique, en hausse de 20%

COPIER LE LIEN

X

FACEBOOK

WHATSAPP

LINKEDIN

E-MAIL

SUDINFO • LAMEUSE

La une | Actualités | Régions | Sports | Vidéos | Max | Programi

ABONNÉS

Un citoyen de Gembloux, arnaqué par un faux site de placements, perd 80.000 euros : « Vous pensez à bien faire pour la famille, à augmenter votre gain, et c'est tout le contraire qui se produit...»

Une plateforme en ligne promet à un habitant de Bossière (Gembloux) des investissements fructueux. Un « engrenage » qui l'a dépouillé de toutes ses économies: 80.000€! Il souhaite se battre pour récupérer son argent.

franceinfo:

Recherche | Direct TV | Direct radio | Live | Services | Mon

Accueil | Menu | Enquêtes | Vrai ou faux | Festival de Cannes 2025 | Fin de vie | Guerre en Ukraine

:témoignage

"Ça a été extrêmement violent" : un chef d'entreprise haut-savoyard victime d'une escroquerie au faux investissement à 1,5 million d'euros

Un vaste réseau international d'escroquerie au faux investissement a été démantelé fin janvier par la gendarmerie. Sept personnes ont été interpellées en France, en Espagne et en Israël. La victime grâce à qui l'enquête a commencé en France prend la parole sur franceinfo.

CENTRE FOR CYBERSECURITY BELGIUM

La fraude à l’investissement
Comment la reconnaître
Comment l’éviter ?

Qu’est-ce que c’est?

- Fraude à l’investissement : l’escroc essaye de soutirer de l’argent à ses victimes en leur offrant un investissement avec un rendement très intéressant. Il s’avère par la suite que l’investissement en question n’existe pas.
- Les signes :
  - **Promesses de gains élevés et garantis**
  - **Pression pour investir vite** (« Opportunité limitée, il faut décider maintenant ! »)
  - **Manque de transparence** sur l’entreprise ou l’intermédiaire
  - **Demande de paiement étrange** : compte étranger, crypto
  - **L’impossibilité de récupérer votre argent** une fois investi

CENTRE FOR CYBERSECURITY BELGIUM

LES 5 PHASES DE LA FRAUDE À L'INVESTISSEMENT

DÉTECTEZ LA FRAUDE AVANT LE CLIC DE TROP

PHASE 1

FAUSSE PUBLICITÉ

Une **publicité farfelue**, **un conseil d'une personnalité** ou un **faux profil** sur les réseaux sociaux. Ces pubs vous dirigent vers de faux sites Internet et de faux experts en investissement.

CONSEIL

Sachez avec qui vous faites affaire.

Vérifiez qui se cache derrière l'entreprise.

PHASE 2

UN INVESTISSEMENT SÛR, DES GAINS ÉLEVÉS

Un **montant initial** sûr (généralement 250 euros) et la promesse de gains rapides et élevés.

CONSEIL

Ne cédez pas à la pression.

Sachez dans quel produit vous investissez.

PHASE 3

DES PROBLÈMES INATTENDUS

Délai d'attente pour retirer votre argent, **frais** et **taxes** imprévus.

CONSEIL

Ne versez plus d'argent

et résiliez votre contrat.

PHASE 4

SILENCE OU HARCÈLEMENT

Vous **ne parvenez plus à joindre** l'entreprise ou à l'inverse, vous êtes **harcelé plusieurs fois** par jour.

CONSEIL

Signalez la fraude

consumerconnect.be

safeonweb.be

et déposez plainte auprès de la police locale.

PHASE 5

NOUVELLE FRAUDE

Un **nouvel interlocuteur** vous contacte. Il prétend vouloir vous aider à récupérer votre investissement... moyennant paiement.

CONSEIL

Ne réagissez jamais à ces offres.

LE SAVIEZ-VOUS

Les Belges ont perdu en 2024 **16,8 millions d'euros** sur les plateformes de trading frauduleuses.

Il s'agit principalement d'escroqueries via des **plateformes de trading** et avec des cryptomonnaies.

Le nombre de cas de **double fraude** augmente.

EN LIGNE, RESTEZ VIGILANT EN INVESTISSANT. DÉCOUVREZ COMMENT SUR SAFEONWEB.BE

Safeonweb.be

Etape 1 : approche de la victime

- Mail, médias sociaux (FB, WhatsApp, ...)
- Publicité sur Internet
- Vol d'identité de personnalité (IA - deepfake)
- Influenceurs
- Fraude à l'investissement sentimentale
- Groupes Whatsapp

Screenshot van de scam die de ronde doet over Michaël Van Droogenbroeck en Bart De Wever


SPEECH
Konbini
ELISE LUCET VS LES INFLUENCEURS

Etape 2 : Diriger les victimes vers des plateformes de trading frauduleuses

CENTRE FOR CYBERSECURITY BELGIUM

➡️ **Mécanisme** : Des sites se font passer pour des plateformes de trading en ligne (forex, actions, cryptos) et promettent des rendements élevés. Après un premier dépôt, les victimes voient des gains fictifs.

➡️ **Signes d'alerte** :

- Rendements garantis irréalistes
- Plateforme non régulée
- Pression pour investir rapidement
- Premier dépôt de 250 € pour tester

Etape 3 : Désillusion

CENTRE FOR CYBERSECURITY BELGIUM

➡️ **Mécanisme** : Des problèmes inattendus apparaissent

- Des délais pour retirer son argent
- Des taxes supplémentaires non prévues qui peuvent aller jusqu'à 30 % de la somme soi-disant gagnée.

Etape 4 : Victimisation

CENTRE FOR CYBERSECURITY BELGIUM

➡️ **Mécanisme** : la victime se rend compte qu'elle s'est fait avoir

- Plus de nouvelles des fraudeurs
- Ou au contraire : harcèlement des victimes avec des dizaines d'appels et de messages par jour.

Etape 5 : Recovery rooms

CENTRE FOR CYBERSECURITY BELGIUM

➡️ **Mécanisme** : après avoir été victime d'une fraude, la personne est contactée par une entreprise qui prétend pouvoir récupérer son argent... moyennant paiement. Il s'agit bien sûr d'une escroquerie.

➡️ **Signaux d'alerte** :

- L'entreprise vous contacte spontanément
- Un paiement est exigé avant que l'argent puisse être récupéré
- Absence d'autorisation officielle

Conséquences pour les victimes

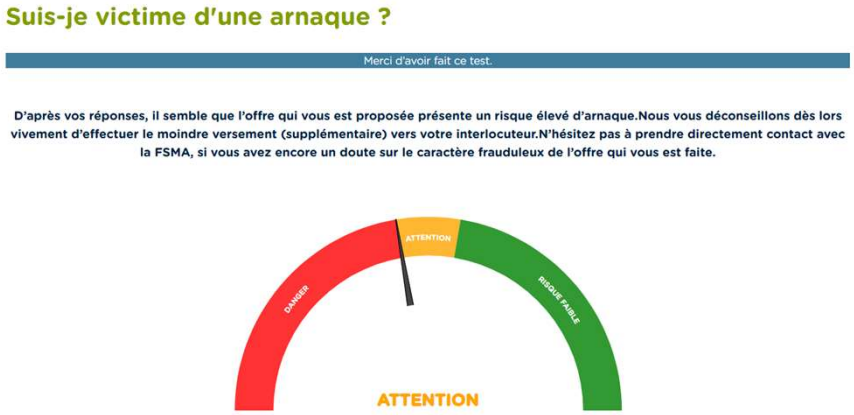
CENTRE FOR CYBERSECURITY BELGIUM

- Perte significative ou totale des économies personnelles
- Difficultés financières pouvant mener à l'endettement
- Conséquences psychologiques : stress, anxiété, perte de confiance, honte
- Conséquences sociales : rupture, isolement, avenir financier incertain pour soi-même et sa famille
- Effet domino : recommandations à des proches qui se font aussi arnaquer

Comment l'éviter

CENTRE FOR CYBERSECURITY BELGIUM

- Soyez critique
- Demandez des informations claires et compréhensibles
- Ne faites pas de paiements précipités
- Protégez vos données personnelles
- Vérifiez le fournisseur – Black list FSMA
- Faites le test
- Un doute ? Contactez la FSMA



Victime?

- Cessez tout contact avec les escrocs
- Cessez tout paiement
- Informez votre banque
- Déposez plainte auprès de la police
- Signalez la fraude
- Méfiez-vous des « recovery rooms »

CENTRE FOR CYBERSECURITY BELGIUM

Chiffres

LES CHIFFRES DE LA FRAUDE À L'INVESTISSEMENT EN LIGNE EN BELGIQUE

(PREMIER SEMESTRE 2025)

CENTRE FOR CYBERSECURITY BELGIUM

37.777,75 €
de perte moyenne par victime belge

65 %
des victimes sont des hommes

14,6 millions €
d'économies disparues

250 €
est souvent proposé comme premier investissement pour « tester » la plateforme

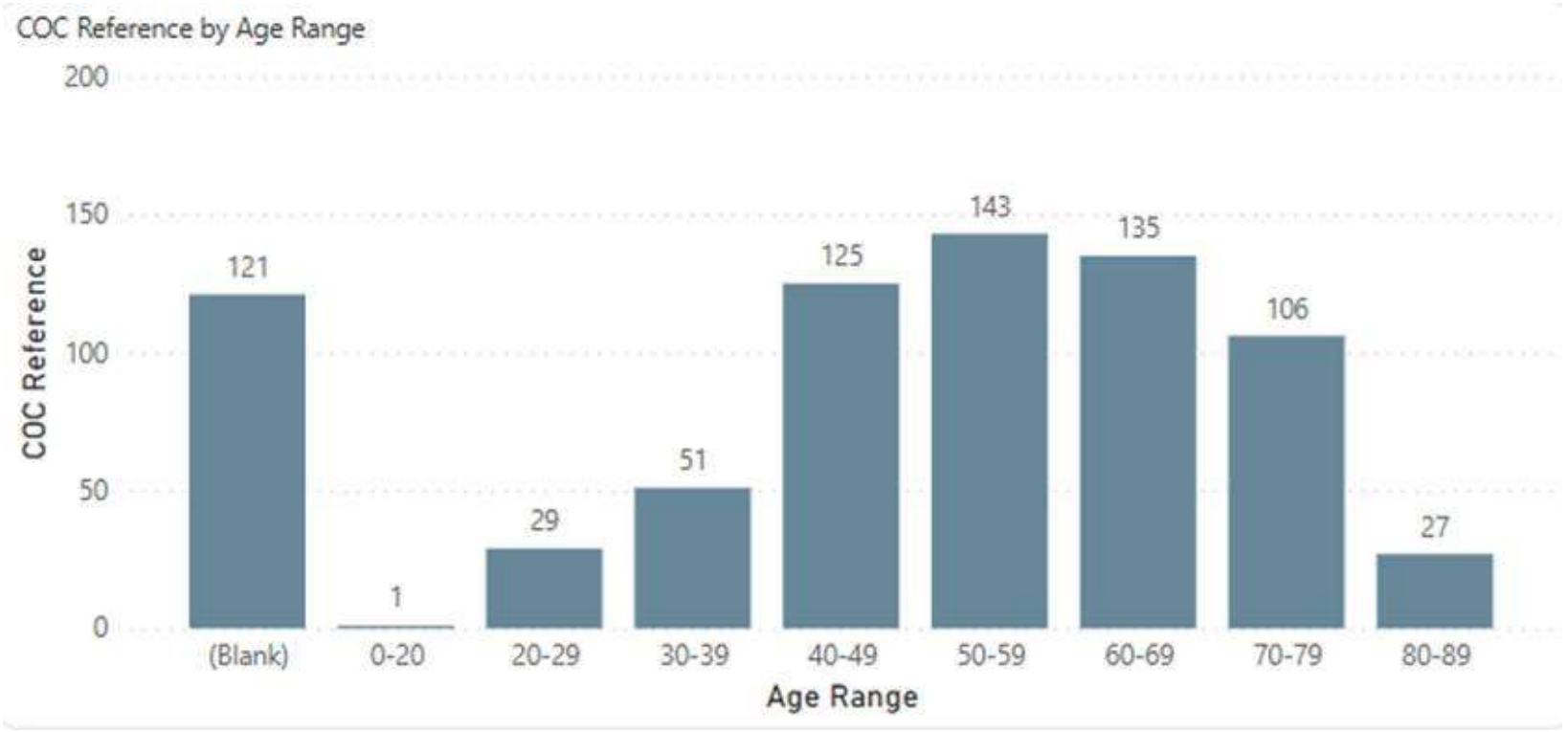
+24 %
de signalements en plus par rapport à 2024

Dark number

CENTRE FOR CYBERSECURITY BELGIUM

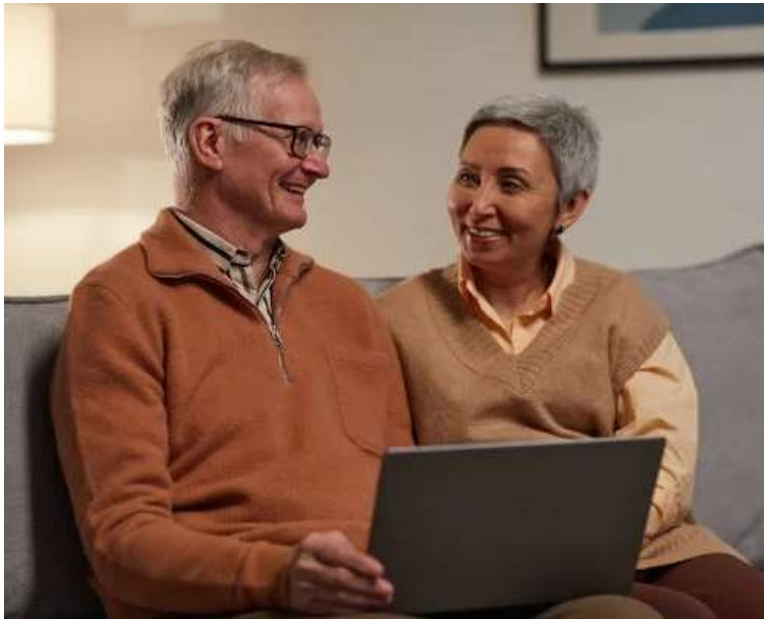
- Chiffre noir élevé : honte, perte de confiance
- Les victimes prennent (dans le meilleur des cas) contact avec leur banque ou la police et moins avec la FSMA

Groupes cibles



Groupes cibles

- Primaire: personnes intéressées par l'investissement (40-70 ans)



- Secondaire: jeunes adultes intéressés dans les cryptos

CENTRE FOR CYBERSECURITY BELGIUM

Campagne Safeonweb 2025

Look and feel

- Animation avec Bill, le sac d’argent
- Testé et validé par un panel de 500 personnes
- Convivial, mais aussi provocateur, sans pour autant susciter la peur
- Toujours positif, en mettant l’accent sur ce qu’il FAUT faire
- Pas de *victim blaming*

Bill

Bill : version jeune adulte

CENTRE FOR CYBERSECURITY BELGIUM

Matériel disponible

Site web Safeonweb

NL FR DE EN

Autres informations et services du gouvernement: www.belgium.be .be

Safeonweb.be

ACTU BLOG CONSEILS @WORK CAMPAGNES OUTILS ENSEIGNER LIENS CONTACT

Ne vous laissez pas piéger par la fraude à l'investissement

L'investissement peut être un moyen intelligent de faire fructifier votre argent, mais il existe malheureusement des fraudeurs qui abusent de votre confiance. La fraude à l'investissement est de plus en plus fréquente, surtout en ligne, et peut entraîner d'énormes pertes financières. Pour les victimes, les conséquences émotionnelles et psychosociales ne sont pas non plus à sous-estimer.

Qu'est-ce que la fraude à l'investissement ?

La fraude à l'investissement est une forme d'escroquerie où des criminels tentent de vous convaincre d'investir de l'argent dans des produits financiers inexistants ou faux (crypto, forex,...). Ils promettent souvent des rendements élevés avec peu de risques, mais en réalité il s'agit d'un piège pour voler votre argent. Souvent, ces fraudeurs disparaissent sans laisser de trace après avoir reçu votre argent.

Affiche


EN LIGNE,
RESTEZ VIGILANT
EN INVESTISSANT
DÉTECTEZ LA FRAUDE
AVANT LE CLIC DE TROP
DÉCOUVREZ COMMENT SUR SAFEONWEB.BE
Safeonweb.be

Folder

LA FRAUDE À L'INVESTISSEMENT, C'EST QUOI ?

Il devient de plus en plus facile d'investir soi-même. Et les fraudeurs en profitent toujours plus. Ils essaient de vous convaincre d'investir votre argent dans des produits financiers fictifs ou mensongers.

Leurs sites Internet et leurs plateformes semblent professionnels et fiables, ils utilisent l'intelligence artificielle avec finesse et leurs « conseillers financiers » ont l'air crédibles. Ce qui rend la fraude à l'investissement en ligne plus difficile à déceler que jamais. Même les investisseurs chevronnés tombent dans le piège avec de lourdes conséquences financières et émotionnelles.

SOYEZ PLUS MALINS QUE LES ESCROCS EN SUIVANT CES CONSEILS :

Une proposition tombée de nulle part ?
Vous recevez un coup de téléphone, un mail ou un message via les réseaux sociaux ? Soyez encore plus vigilants !

Passez votre interlocuteur au crible
Est-il agréé ou figure-t-il sur une liste noire ?

Restez critique
Vous recevez une offre aussi intéressante qu'inattendue ? Ne tombez pas dans le piège. Restez calme. Réfléchissez. Posez des questions.

Comprenez dans quoi vous investissez
Le produit n'est pas clair ou les explications manquent de précision ? Alors, c'est risqué.

Pas de pression
Ne faites pas de paiement dans la précipitation. Prenez le temps d'analyser l'offre.

Protégez vos données personnelles
Ne communiquez jamais vos données d'identité ou vos coordonnées bancaires sans réfléchir.

Une demande de paiement étrange ?
Vous devez transférer de l'argent vers un compte étranger ou via la cryptomonnaie ? Alerte !

VERIFIEZ SUR FSMA.BE

Infographie

CENTRE FOR CYBERSECURITY BELGIUM

LES 5 PHASES DE LA FRAUDE À L'INVESTISSEMENT

DÉTECTEZ LA FRAUDE AVANT LE CLIC DE TROP

PHASE 1

FAUSSE PUBLICITÉ

Une **publicité farfelue**, **un conseil d'une personnalité** ou un **faux profil** sur les réseaux sociaux. Ces pubs vous dirigent vers de faux sites Internet et de faux experts en investissement.

CONSEIL

Sachez avec qui vous faites affaire.

Vérifiez qui se cache derrière l'entreprise.

PHASE 2

UN INVESTISSEMENT SÛR, DES GAINS ÉLEVÉS

€250

Un **montant initial** sûr (généralement 250 euros) et la promesse de gains rapides et élevés.

CONSEIL

Ne cédez pas à la pression.

Sachez dans quel produit vous investissez.

PHASE 3

DES PROBLÈMES INATTENDUS

Délai d'attente pour retirer votre argent, **frais** et **taxes** imprévus.

CONSEIL

Ne versez plus d'argent

et résiliez votre contrat.

PHASE 4

SILENCE OU HARCÈLEMENT

Vous **ne parvenez plus à joindre** l'entreprise ou à l'inverse, vous êtes **harcelé plusieurs fois** par jour.

CONSEIL

Signalez la fraude

consumerconnect.be

safeonweb.be

et déposez plainte auprès de la police locale.

PHASE 5

NOUVELLE FRAUDE

Un **nouvel interlocuteur** vous contacte. Il prétend vouloir vous aider à récupérer votre investissement... moyennant paiement.

CONSEIL

Ne réagissez jamais à ces offres.

LE SAVIEZ-VOUS

Les Belges ont perdu en 2024 **16,8 millions d'euros** sur les plateformes de trading frauduleuses.

Il s'agit principalement d'escroqueries via des **plateformes de trading** et avec des cryptomonnaies.

Le nombre de cas de **double fraude** augmente.

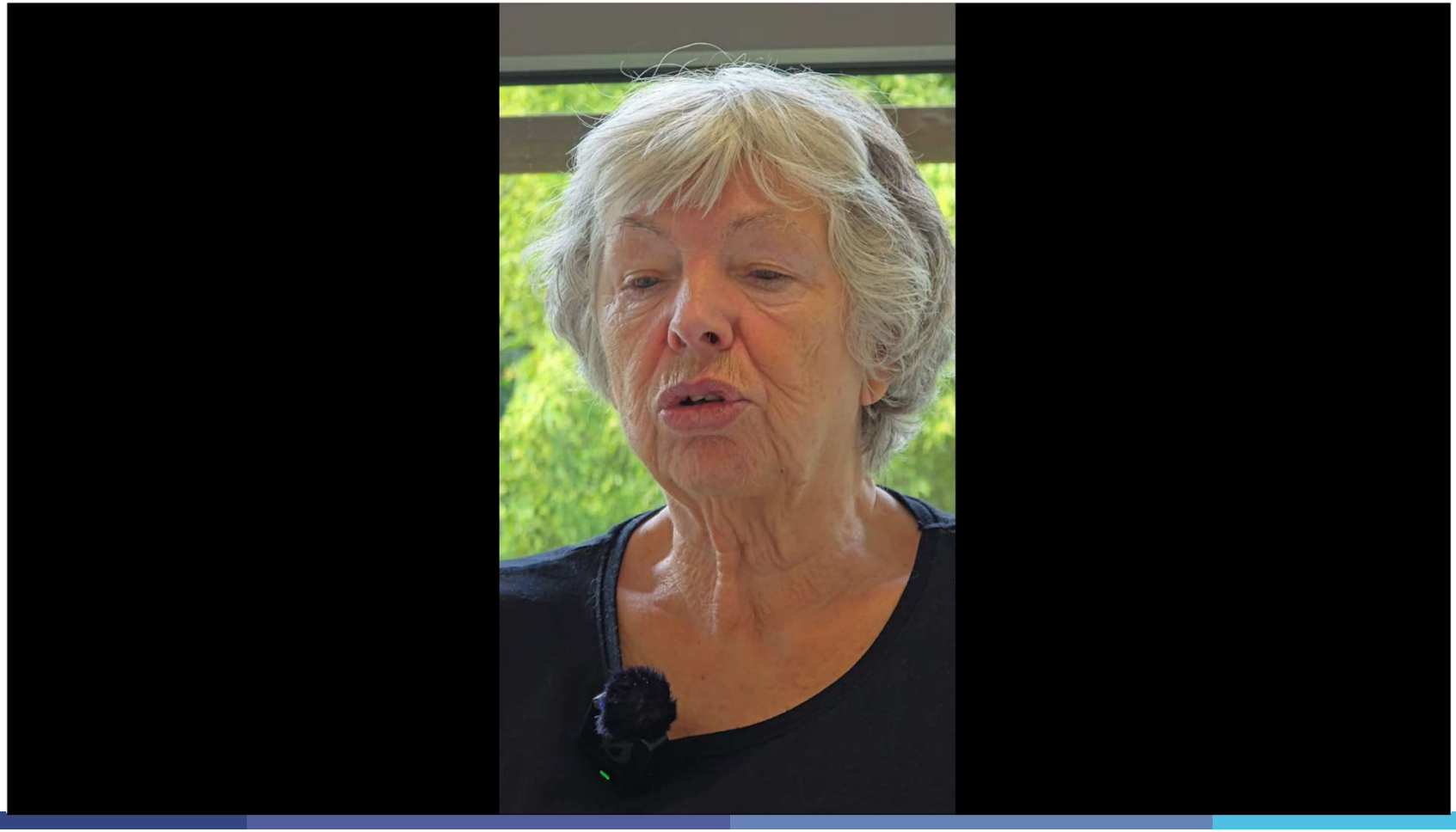
EN LIGNE, RESTEZ VIGILANT EN INVESTISSANT. DÉCOUVREZ COMMENT SUR SAFEONWEB.BE

Safeonweb.be

Goodie : billet à gratter

Témoignages

CENTRE FOR CYBERSECURITY BELGIUM



Témoignages

CENTRE FOR CYBERSECURITY BELGIUM

Modalités pratiques

CENTRE FOR CYBERSECURITY BELGIUM

- Disponible sur https://safeonweb.be/fr/materiel-de-campagne
- Tout le matériel peut être utilisé, partagé, distribué à des fins non commerciales et sous réserve de la mention de la source (Safeonweb)

CENTRE FOR CYBERSECURITY BELGIUM

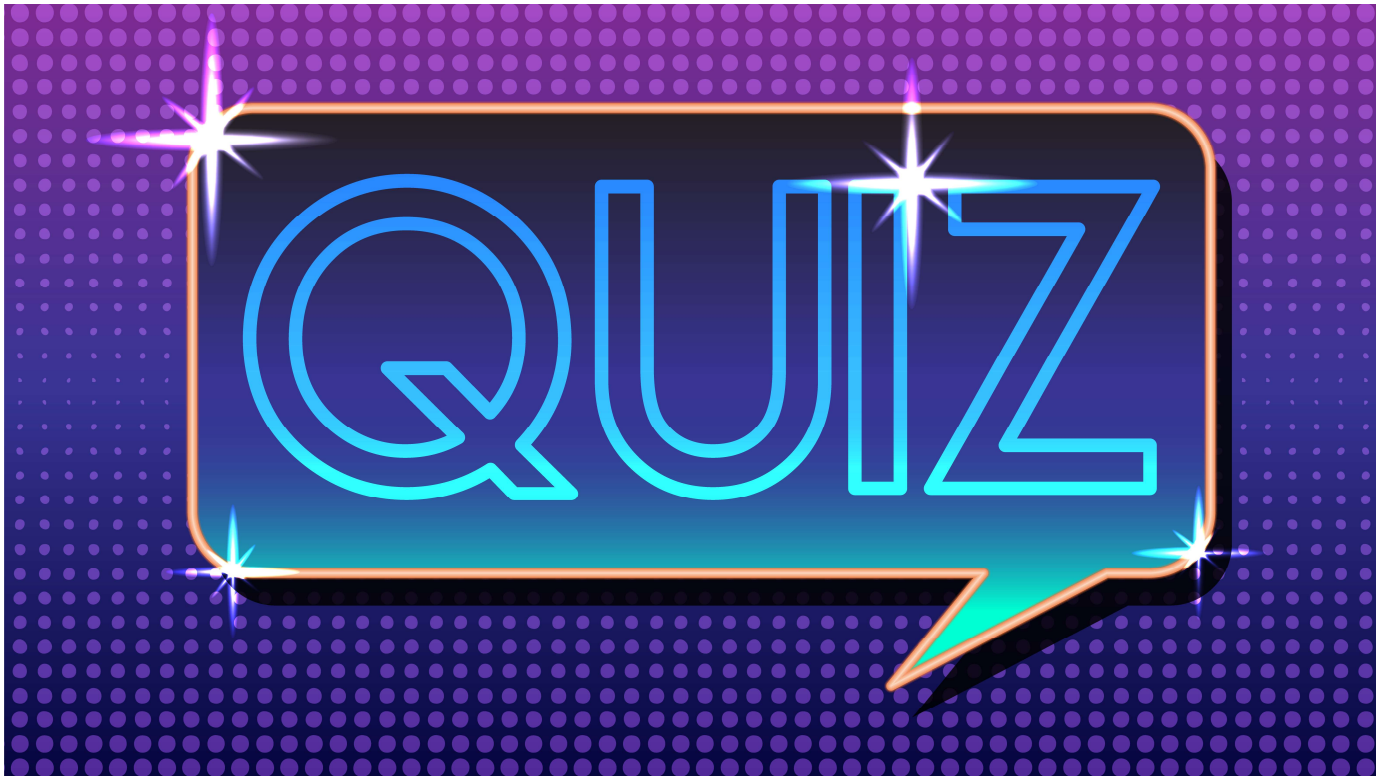
Le phishing

Phishing

CENTRE FOR CYBERSECURITY BELGIUM

- Qu’est-ce que c’est?
  - Escroquerie en ligne
  - A l'aide de mails, SMS, messages WhatsApp
- Renvoient vers
  - Faux site Internet
  - Annexe suspecte
  - Application à télécharger
- Objectif : récupérer les données bancaires de la victime

CENTRE FOR CYBERSECURITY BELGIUM



Comment reconnaître un message frauduleux ?

CENTRE FOR CYBERSECURITY BELGIUM

Les différentes formes

CENTRE FOR CYBERSECURITY BELGIUM

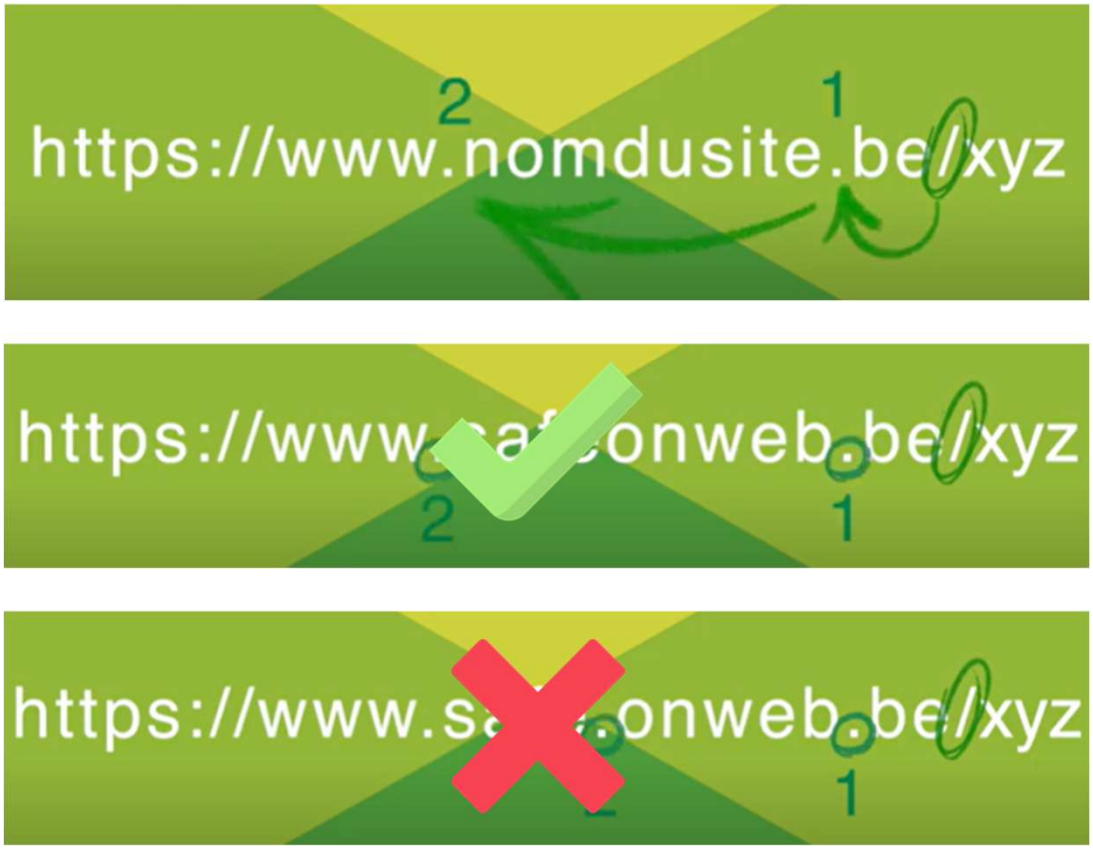
- Phishing :
  - Mail
- Smishing :
  - SMS
- Vishing :
  - Téléphone
  - Voice + phishing

Les différentes formes

CENTRE FOR CYBERSECURITY BELGIUM

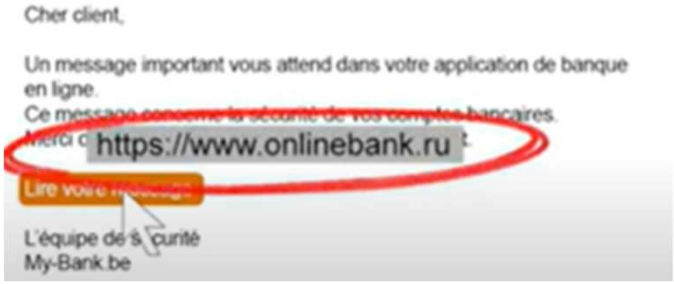
- Quishing :
  - code QR
- Angler phishing :
  - sur les réseaux sociaux
  - fraudeurs se font passer pour le service clientèle

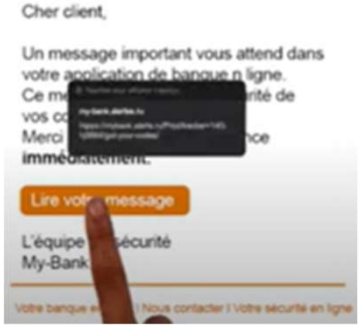
Comment lire un lien?



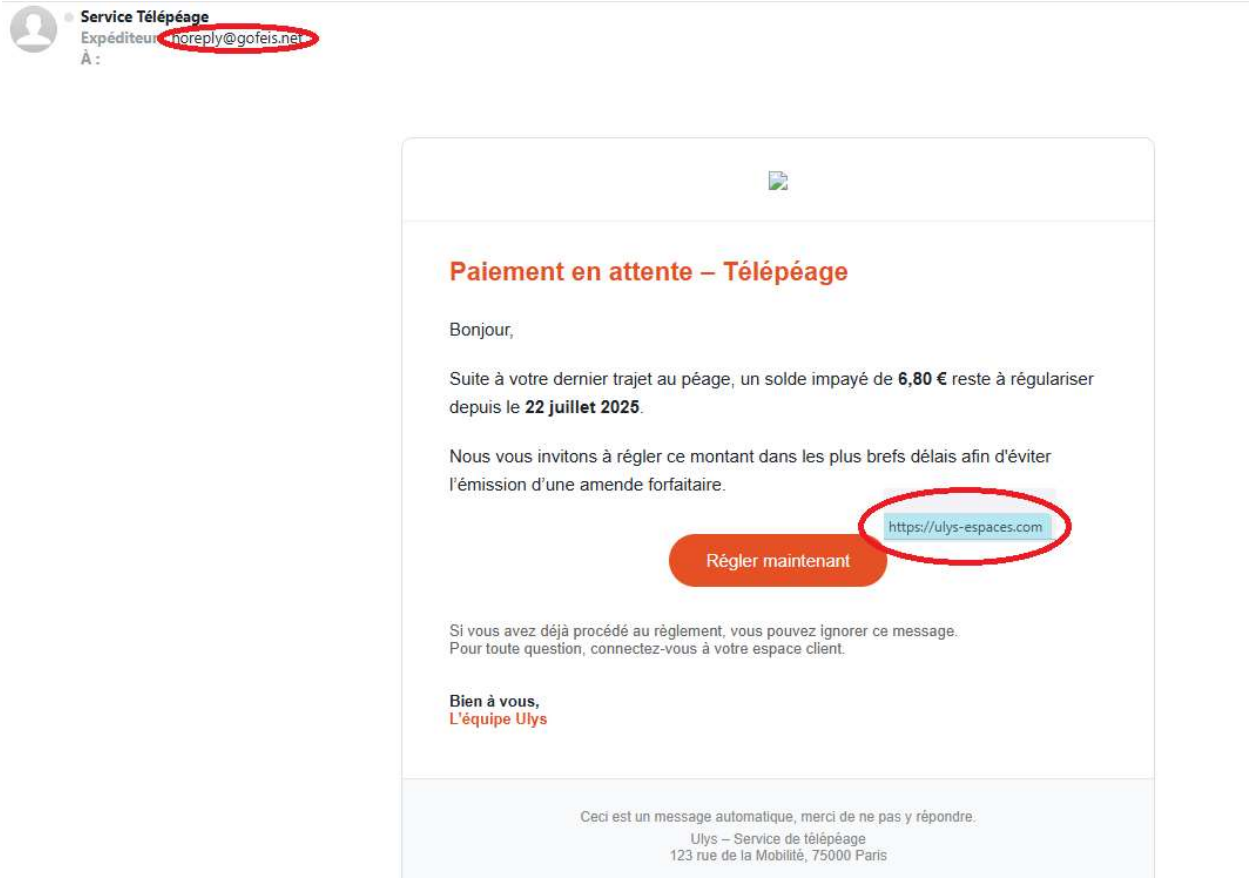
Comment savoir où le lien renvoie?

- SMS / Whatsapp
- Attention aux réducteurs d'URL : Bitly, TinyURL, ...
- Ordinateur
- Smartphone/tablette





Quelques exemples



Service Télépéage
Expéditeur : noreply@gofeis.net
À :

Paiement en attente – Télépéage

Bonjour,

Suite à votre dernier trajet au péage, un solde impayé de **6,80 €** reste à régulariser depuis le **22 juillet 2025**.

Nous vous invitons à régler ce montant dans les plus brefs délais afin d'éviter l'émission d'une amende forfaitaire.

https://ulys-espaces.com

Régler maintenant

Si vous avez déjà procédé au règlement, vous pouvez ignorer ce message.
Pour toute question, connectez-vous à votre espace client.

Bien à vous,
L'équipe Ulys

Ceci est un message automatique, merci de ne pas y répondre.
Ulys – Service de télépéage
123 rue de la Mobilité, 75000 Paris

Quelques exemples

CENTRE FOR CYBERSECURITY BELGIUM

De : Partenamut <remboursement@undervisionsewercamera.com>
Envoyé : mardi 14 octobre 2025 15:02
À : [redacted]
Objet : Action requise : Confirmez votre remboursement

Un remboursement de 180 € a été enregistré sur votre compte.

FAKE

Avis concernant un remboursement

Madame, Monsieur,

Nous vous informons qu'un remboursement d'un montant de **180,00 €** a été enregistré sur votre compte affilié à **Partenamut**.

Pour finaliser l'opération et vérifier vos coordonnées bancaires, veuillez cliquer sur le lien ci-dessous et confirmer les informations requises.

Confirmer les informations

Cette opération ne pourra être validée qu'après confirmation de votre part. Nous vous remercions de votre réactivité.

Quelques exemples

CENTRE FOR CYBERSECURITY BELGIUM

-------- Doorgestuurd bericht --------
Onderwerp: Votre Colissimo Arrive!
Datum:
Van: Re <no-reply@krjgfvl.sfr.fr>
Aan:

FedEx

A package addressed to you just arrived at our local dispatch facility.

However, ther was mismtach of adress due to logistic handling at our end.

We urge you to kindly update our adress system with your adress to enable us get your package accross.

ADRESS VERIFICATION SYSTEM

We hope to get your package accross before the end of the business day

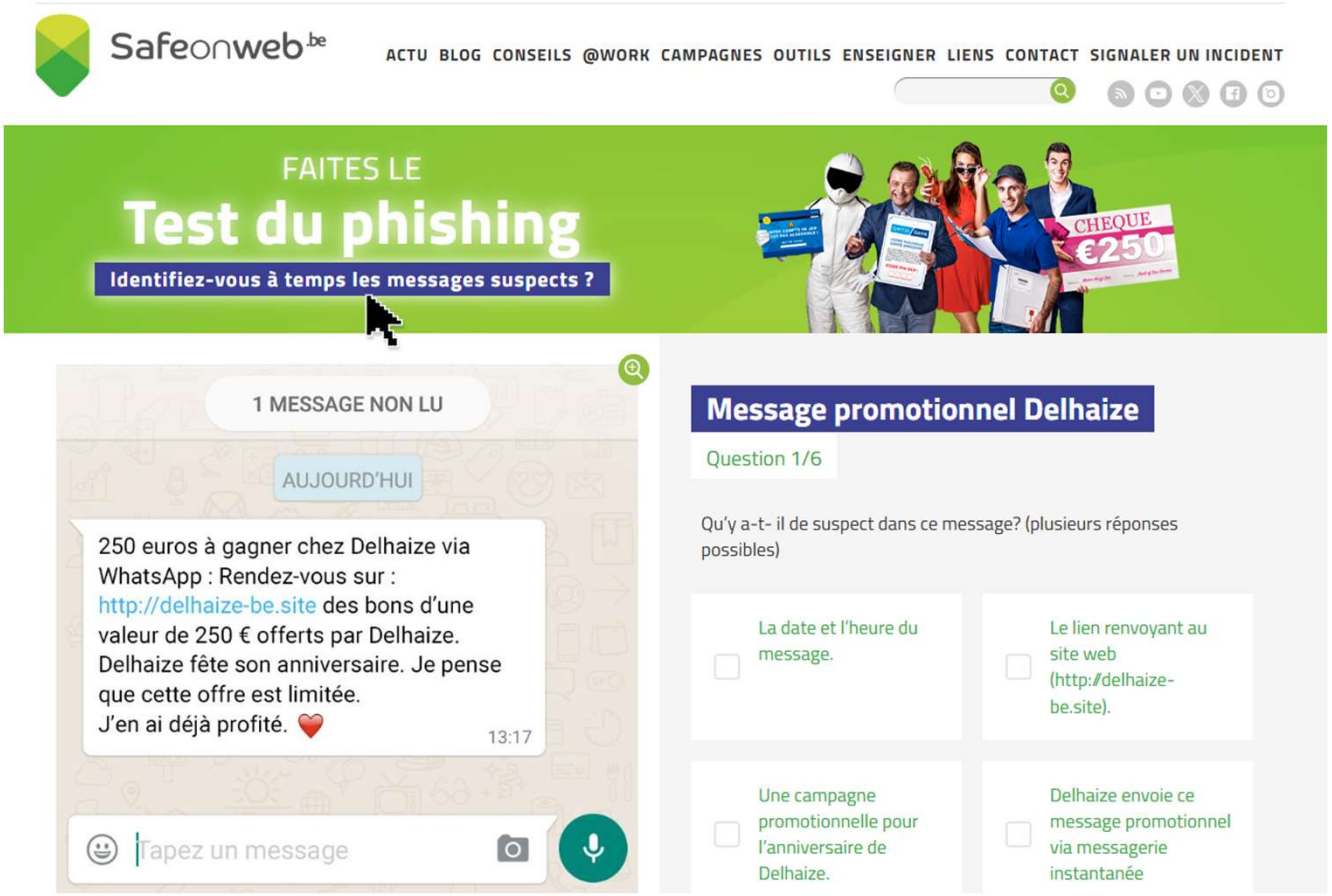
Sincerelyy

Package Dispatch Manager

Nous espérons que vous apprécierez recevoir ce message. Toutefois, si vous ne souhaitez pas recevoir de futurs e-mails.
Veuillez vous désabonner ici.

Test du phishing

CENTRE FOR CYBERSECURITY BELGIUM



Trop tard, j'ai cliqué…

CENTRE FOR CYBERSECURITY BELGIUM

- Card Stop : 078/170 170
- Banque : bloquer paiement ou compte
- Plainte police
- Changez vos mots de passe
- Prévenez vos contacts
- Scan antivirus
- Transférez le message à suspect@safeonweb.be

Quelques chiffres

CENTRE FOR CYBERSECURITY BELGIUM

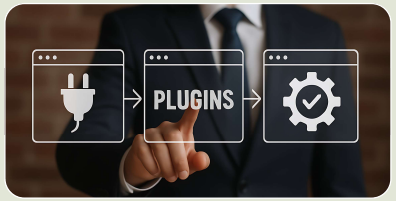
- 69 % des Belges ont reçu au moins un message de phishing au cours des 6 derniers mois
- 8 % des Belges se disent avoir été victimes de phishing
- 83% pensent savoir reconnaître un mail suspect
- 23 % des jeunes (16-30 ans) n'ont jamais entendu parler de phishing
- Seul 62 % des victimes savaient comment réagir
- 32 % des Belges ne savent pas comment reconnaître un site suspect

Safeonweb.be @home

CENTRE FOR CYBERSECURITY BELGIUM

Les outils

L’appli Safeonweb



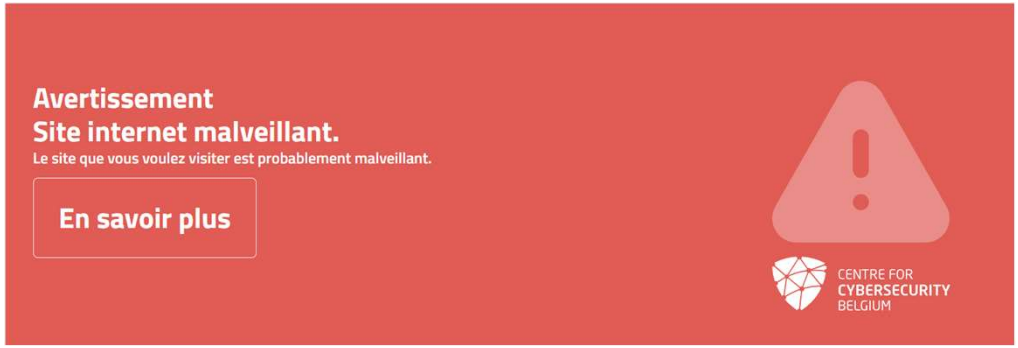
L’extension de navigateur Safeonweb

Surfez sans souci

Suspect@ safeonweb.be

suspect@safeonweb.be

CENTRE FOR CYBERSECURITY BELGIUM

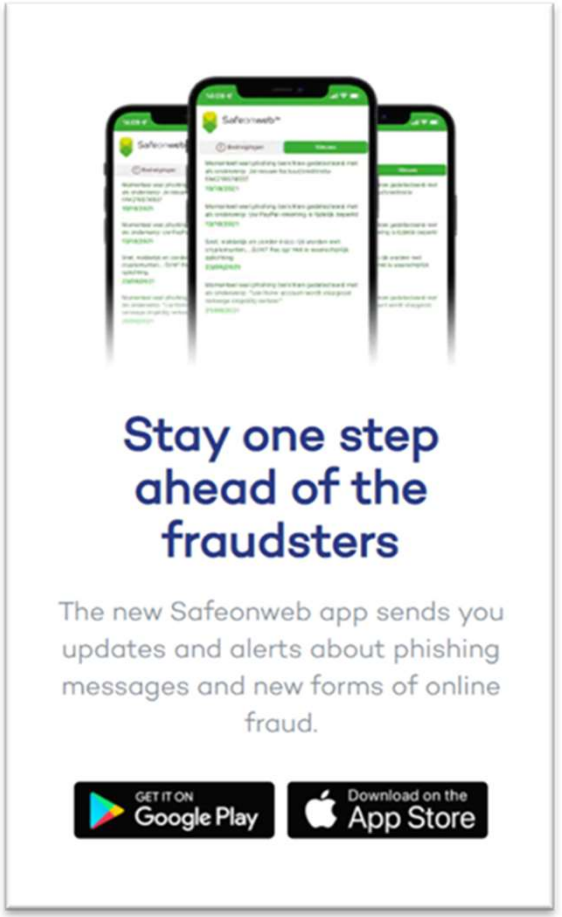


suspect@safeonweb.be

App Safeonweb

CENTRE FOR CYBERSECURITY BELGIUM

- Recueil des informations sur les messages suspects récurrents
- Partage via l'application Safeonweb
- Les citoyens sont rapidement informés des messages suspects qui circulent



E-learning : Surfer sans souci

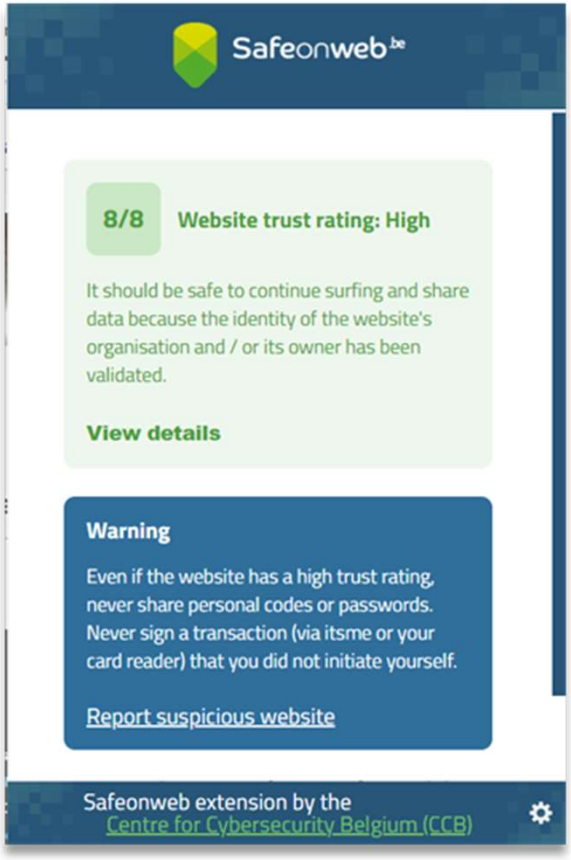
CENTRE FOR CYBERSECURITY BELGIUM

- Phishing: regarde où tu vas!
- Authentification à deux facteurs : sécurisez vos comptes en ligne
- Escroquerie : Vérifie avant de transférer de l'argent
- Fraude à l'investissement : à suivre

Extension de navigateur Safeonweb

CENTRE FOR CYBERSECURITY BELGIUM

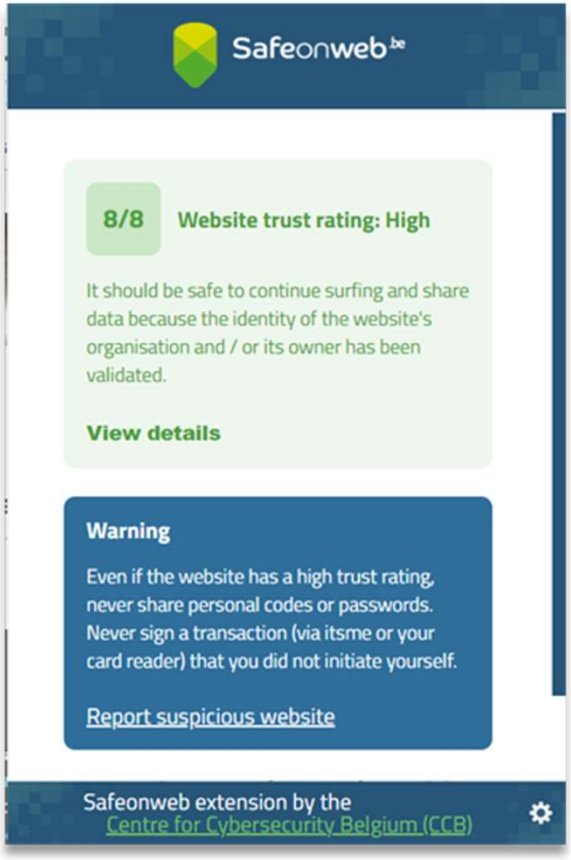
- Aide à évaluer la fiabilité de chaque site web visité
- L'extension attribue un niveau de confiance à chaque site web
  - Vert : le site web est sûr, vous pouvez naviguer en toute tranquillité.
  - Orange : Le propriétaire de ce site ne peut pas être vérifié. Vous pouvez visiter ce site, mais n'y introduisez pas de données personnelles.
  - Rouge : Arrêtez immédiatement, ce site n'est pas sûr et peut être dangereux.



Extension de navigateur Safeonweb

CENTRE FOR CYBERSECURITY BELGIUM

- Pas de surveillance : données anonymisées
- Disponible uniquement sur desktop et laptop
- Google Chrome, Microsoft Edge, Opera, Vivaldi, Brave, etc.
- Ne remplace pas un antivirus



Extension de navigateur Safeonweb - installation

CENTRE FOR CYBERSECURITY BELGIUM

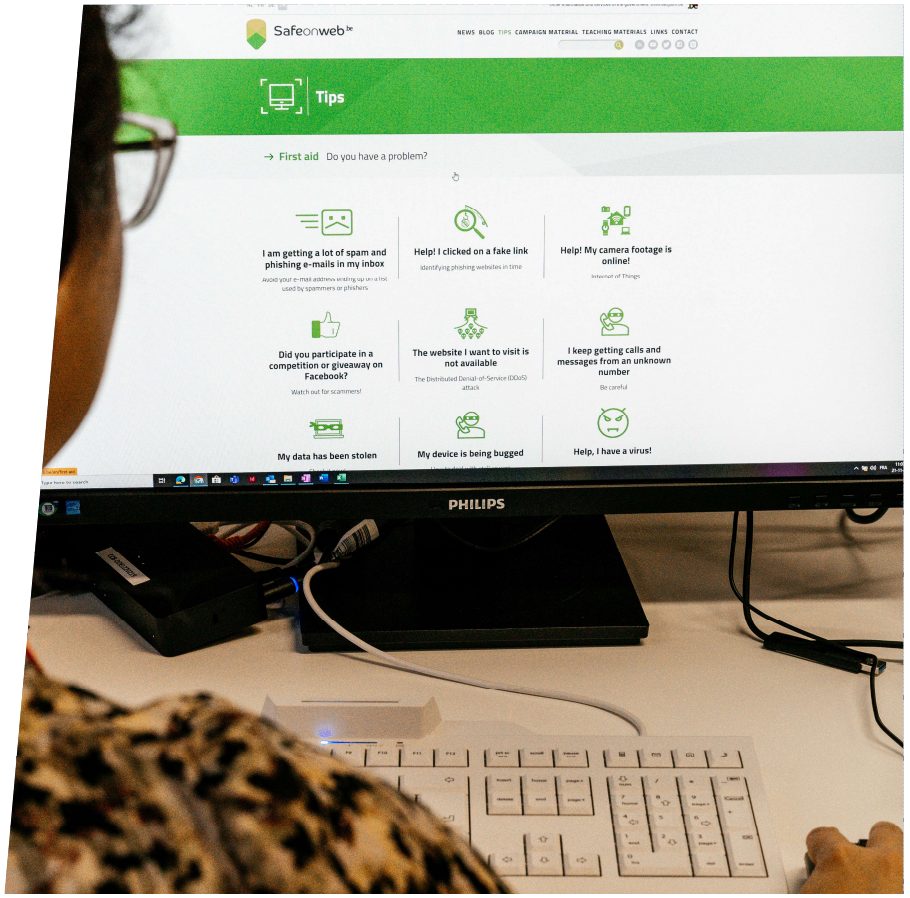
- Ouvrez le Chrome Web Store en suivant ce lien : https://chrome.google.com/webstore/category/extensions
- Recherchez l'extension Safeonweb dans la boutique.
- Cliquez sur le bouton "Ajouter à Chrome".
- Cliquez sur le bouton "Ajouter une extension" dans la fenêtre contextuelle.
- Sélectionnez la pièce de puzzle dans le coin supérieur droit de votre navigateur et épinglez l'extension Safeonweb.
- L'icône Safeonweb apparaîtra à droite de la barre d'adresse. Sa couleur changera en fonction du niveau de confiance du site web que vous visitez.

Safeonweb.be @home

CENTRE FOR CYBERSECURITY BELGIUM

Le site web

- Actu/Alertes de la semaine
- Conseils et astuces sur la sécurité en ligne
- Au secours : avez-vous un problème ?
- Test pour connaitre son niveau de sécurité en ligne
- Matériel de campagne
- Matériel pédagogique
- Liens intéressants



Suivez-nous

CENTRE FOR CYBERSECURITY BELGIUM

	Facebook - Safeonweb.be
	Instagram - Safeonweb.be
	X - @safeonweb_be
	BlueSky - @safeonweb-be.bsky.social
	YouTube - @safeonwebbe

Contactez nous

CENTRE FOR CYBERSECURITY BELGIUM

- L'équipe de Safeonweb
  comm@ccb.belgium.be
- Cathy Grimmeau
  cathy.grimmeau@ccb.belgium.be
- Katrien Eggers
  katrien.eggers@ccb.belgium.be

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

.be