

# La cybersécurité en Belgique

## Présentation du CCB et introduction sur les cybermenaces

---

V1.1: Janvier 2022 Le Centre pour la Cybersécurité Belgique



## Vue d'ensemble

---

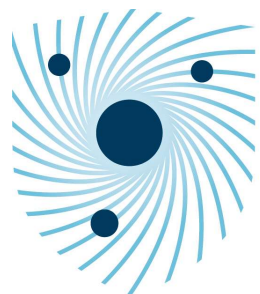
1. Présentation du Centre pour la Cybersécurité Belgique
2. Phishing
3. Arnaque/fraude en ligne
  - Focus case : Microsoft scam
  - Focus case : fraude au CEO
  - Focus case : Sextorsion scam
4. Malware
  - Focus case : ransomware
5. Piratage de compte
  - Focus case : piratage IOT
6. Conclusion

# 1.

## Présentation du Centre pour la Cybersécurité Belgique

## Qu'est-ce que le Centre pour la Cybersécurité Belgique ?

---



CENTRE FOR  
**CYBER SECURITY**  
BELGIUM



**CERT.be**  
The Federal Cyber Emergency Team



**Safeonweb**.be

**Différence avec la FCCU ? = Federal Computer Crime Unit (Police fédérale)**

## Objectif

---



Faire de la Belgique l'un  
des pays les moins  
vulnérables d'Europe


## Mission :

---

- superviser et coordonner
- différents projets relatifs à la cybersécurité
- la coordination
- cadre réglementaire
- gestion de crise
- standards, directives et normes de sécurité
- la représentation belge dans les forums internationaux
- l'évaluation et la certification
- Informer et sensibiliser


# www.ccb.belgium.be

NL DE EN Autres informations et services officiels : [www.belgium.be](http://www.belgium.be) **.be**




Rechercher

Home Actualités Organisation Secteurs - Offres d'emploi Contact




**At Home**

Le site safeonweb.be a pour ambition d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique.




**At Work**

Pour plus d'informations, des conseils et des liens utiles sur la protection de vos ordinateurs et réseaux au travail.




**At School**

Pour plus d'information sur les formations, le matériel pédagogique et la sécurité informatique à l'école.




**At government**

Lignes directrices pour les différents systèmes d'information des organismes publics. Formations pour les fonctionnaires fédéraux.



**Vital Sectors**

Différents projets qui protègent les secteurs vitaux en Belgique contre les cyberattaques




**CERT.be**

CERT.be est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB) et fournit des services dans le domaine de la cybersécurité

NL DE EN Autres informations et services officiels : [www.belgium.be](http://www.belgium.be) **.be**

NL DE EN Autres informations et services officiels : [www.belgium.be](http://www.belgium.be) **.be**



Rechercher

Home Actualités Organisation Secteurs - Offres d'emploi Contact



**At Home**

Le site safeonweb.be a pour ambition d'informer rapidement et efficacement les citoyens belges en matière de sécurité informatique.




**At Work**

Pour plus d'informations, des conseils et des liens utiles sur la protection de vos ordinateurs et réseaux au travail.



**At School**

Pour plus d'information sur les formations, le matériel pédagogique et la sécurité informatique à l'école.



**At government**

Lignes directrices pour les différents systèmes d'information des organismes publics. Formations pour les fonctionnaires fédéraux.



**Vital Sectors**

Différents projets qui protègent les secteurs vitaux en Belgique contre les cyberattaques



**CERT.be**

CERT.be est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB) et fournit des services dans le domaine de la cybersécurité

NL DE EN Autres informations et services officiels : [www.belgium.be](http://www.belgium.be) **.be**

# www.CERT.be

NL FR DE EN Other official information and services: [www.belgium.be](http://www.belgium.be)

Rechercher

[À propos](#) [Signaler un incident](#) [Conseils](#) [Actualités](#) [Offres d'emploi](#) [Contact](#)

### Bienvenue sur le site du CERT.be

La Computer Emergency Response Team fédérale, ou CERT.be, est le service opérationnel du Centre pour la Cybersécurité Belgique (CCB). Le CERT.be est chargé de détecter, d'observer et d'analyser les problèmes de sécurité en ligne ainsi que d'informer notre audience à ce propos.

BESOIN DE CONSEILS OU D'AIDE LORS D'UN INCIDENT?NOUS AIDONS LES HÔPITAUX EN CAS DE CYBERINCIDENT

#### CONSEILS ET AVERTISSEMENTS RÉCENTS

 <p><b>LES CYBERCRIMINELS EXPLOITENT LES BOÎTES MAIL D'ENTREPRISES BELGES POUR VOLER DES MOTS DE PASSE</b></p> <p>Wed, 03/02/2021 - 20:09</p> <p>Plusieurs partenaires en charge de la cybersécurité font état d'attaques visant des entreprises belges.</p>	 <p><b>LES VULNÉRABILITÉS POUR DNSPOOQ ET DNSMASQ PRÉSENTENT UN RISQUE D'EMPOISONNEMENT DU CACHE DNS POUR LES PÉRIPHÉRIQUES RÉSEAU ET LES DISTRIBUTIONS LINUX</b></p> <p>21/01/2021</p> <ul style="list-style-type: none"><li>Le CERT.be recommande aux utilisateurs de mettre leur logiciel à jour pour passer à</li></ul>	 <p><b>LE PARE-FEU ZYXEL ET LES CONTRÔLEURS DE POINTS D'ACCÈS (AP) CONTIENNENT DES UTILISATEURS/MOTS-DE-PASSE VULNÉRABLES</b></p> <p>07/01/2021</p> <p>* CERT.be recommande de mettre à jour le firmware du pare-feu Zyxel à la version "ZLD V4.60 Patch1".</p>
--	--	---



# www.CERT.be

NL FR DE EN Other official information and services: [www.belgium.be](http://www.belgium.be)

  [Rechercher](#)

[À propos](#) [Signaler un incident](#) [Conseils](#) [Actualités](#) [Offres d'emploi](#) [Contact](#)

## SIGNALER UN INCIDENT



### Premiers secours en cas de cyberattaque

Vous êtes victime d'une cyberattaque et vous pensez qu'elle est toujours en cours ? [Tentez alors de suivre les étapes suivantes.](#)



### Formulaire de signalement

Je suis : un utilisateur particulier, une entreprise, un service public, une organisation (sans but lucratif) ou un opérateur d'importance vitale.

[Je souhaite signaler un incident ou recevoir de l'aide lors d'un incident.](#)



### Signalement par e-mail

Je souhaite envoyer un e-mail à CERT.be : utilisez l'adresse [cert\[at\]cert.be](mailto:cert[at]cert.be).

Je souhaite [envoyer un e-mail crypté](#) à CERT.be.

Vous souhaitez échanger des informations en toute sécurité ?

[Utilisez le protocole Traffic Light Protocol \(TLP\)](#)

Je suis un opérateur de services essentiels qui n'est pas soumis au contrôle de la Banque nationale de Belgique ou un fournisseur de services numériques et je veux signaler un incident NIS.



### Signaler un message suspect

J'ai reçu un message suspect et je souhaite le signaler. Transférez le message à [suspect\[at\]safeonweb.be](mailto:suspect[at]safeonweb.be).

[Plus d'informations sur les messages suspects](#)

# www.safeonweb.be

NL FR DE EN Autres informations et services du gouvernement: [www.belgium.be](http://www.belgium.be) .be

**Safeonweb.be** ACTUALITÉ BLOG CONSEILS MATÉRIEL DE CAMPAGNE LIENS CONTACT

---

## Les mots de passe, c'est dépassé.

Découvrez la campagne





**Au secours**  
Avez-vous un problème?



**Testez votre sécurité**  
Faites nos tests !



**Surfez en toute sécurité**  
Conseils pour surfer en toute sécurité

**⚠ Risques actuels**

- 20 jan 2021: La police met en garde contre le phishing ...
- 10 déc 2020: Les SMS suspects peuvent désormais ...
- 07 déc 2020: Un appel manqué d'un numéro étranger ? ...
- 23 nov 2020: Febelfin met en garde contre la fraude ...
- 06 nov 2020: De plus en plus de fraude au CEO: soyez ...
- 28 oct 2020: Méfiez-vous des messages de hameçonnage ...
- 24 oct 2020: De plus en plus de notifications d'escroqueries ...
- 22 oct 2020: Gare à la « fraude aux comptes à sécurité ...

NL FR DE EN Autres informations et services du gouvernement: [www.belgium.be](http://www.belgium.be) .be

**Safeonweb.be** ACTUALITÉ BLOG CONSEILS MATÉRIEL DE CAMPAGNE LIENS CONTACT

---

## Les mots de passe, c'est dépassé.

Découvrez la campagne





**Au secours**  
Avez-vous un problème?



**Testez votre sécurité**  
Faites nos tests !



**Surfez en toute sécurité**  
Conseils pour surfer en toute sécurité

**⚠ Risques actuels**

- 20 jan 2021: La police met en garde contre le phishing ...
- 10 déc 2020: Les SMS suspects peuvent désormais ...
- 07 déc 2020: Un appel manqué d'un numéro étranger ? ...
- 23 nov 2020: Febelfin met en garde contre la fraude ...
- 06 nov 2020: De plus en plus de fraude au CEO: soyez ...
- 28 oct 2020: Méfiez-vous des messages de hameçonnage ...
- 24 oct 2020: De plus en plus de notifications d'escroqueries ...
- 22 oct 2020: Gare à la « fraude aux comptes à sécurité ...

**Lokale Politie Gent** @GentseFlikken 20h

Wees op je hoede voor phishing mails. Denk twee keer na voor je op een link klikt. Herken verdachte berichten en stuur ze door naar [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be). #preventiehelpt @safeonweb\_be Meer tips vind je op [safeonweb.be/index.php/nl/t...](http://safeonweb.be/index.php/nl/t...)



Lokale Politie Gent Retweeted

**Politie Brugge** @PolitieBrugge 23h

Mail van onbekende afzender in je inbox? Open geen bijlages en klik niet door via een link. Bezorg deze bedenkelijke mail aan [verdacht@safeonweb.be](mailto:verdacht@safeonweb.be) en relax... #CyberSecurity @safeonweb\_be



Bel voor dringende politiehulp 101.

**Federale Politie** Nieuws Vragen Opsporingen Over ons Contact

Stadszwaart - Nieuws - Een grote campagne om niet meer in de phishingval te lopen

**Vermist**  
 Help ons bij het terug vinden van vermiste personen. Hebt u tips? Vermiste personen ...

**Gezocht**  
 Help ons bij het zoeken naar daders of slachtoffers van een misdrijf. Gezochte personen ...

**Een grote campagne om niet meer in de phishingval te lopen**  
 Wo 2.10.2019 - 12:50  
 In oktober gaat de sensibiliseringscampagne rond cybeveiligheid van start. Het thema dit jaar is phishing. Onze expert waarschuwt!

"Relax en denk twee keer na voor je op een link klikt." Zo luidt de slogan van de nieuwe preventiecampagne van het Centrum voor Cybersecurity België en de Cyber Security Coalition. Heel de maand oktober ligt de focus op de strijd tegen phishing. Ondanks de herhaaldelijke tips blijven gebruikers op kwaadaardige links klikken. Die 'klikdrang' was de inspiratiebron voor de slogan van de preventiecampagne 2019. Een lachende hippie illustreert de boodschap. "Phishing blijft een groot probleem dat zowel de burger als ondernemingen en overheidsinstaties treft. Op platformen zoals LinkedIn kunnen gebruikers details over hun job delen. Op basis van die info kiezen cybercriminelen hun slachtoffers uit die ingaan op een bericht

**Lanaken-Maasmechelen** 1d

liked a Tweet you were mentioned in

**PZ G'bergenLierde** @PzGbergenLi... 1d

Valse #berichten via #email #SMS #WhatsApp #messenger! #phishing heb je in allerlei vormen! 🗨️ Hoe herken je ze en wat doe je wel of niet? Loop niet in de val! #cybercrime #geraardsbergen #lierde @safeonweb\_be youtube.com/watch?v=HwnJxY...



**Politie Bilzen-Hoeselt-Riemst** heeft een bericht gedeeld.  
 1 oktober om 19:37

Ontdek hier de nieuwe campagne van safeonweb.be!



Bel voor dringende politiehulp 101. Geen spoed, wel politie? Bel 02 769 69 30.

**Lokale Politie** Druivenstreek Nieuws Vragen Verkeer Over ons Contact

Stadszwaart - Nieuws - Relax En denk twee keer na voor je op een link klikt.

**Internetmisdrijven**  
 Bescherm uzelf voldoende tegen de toenemende gevaren op het internet! Misdrijven op het internet ...

**Maak een afspraak**  
 Vanaf 02 mei 2019 werkt de lokale politie met een online afsprakenbeheer. Maak een afspraak ...

**Relax! En denk twee keer na voor je op een link klikt.**  
 Di 1.10.2019 - 12:03  
 In het kader van de European Cyber Security Month lanceert het Centre for Cyber Security Belgium een sensibiliseringscampagne rond cybeveiligheid. Thema dit jaar is phishing, met als hoofdboodschap "denk 2x na voor je op een link klikt."

Hoe herken je verdachte phishing berichten?  
 • Ontwaakt en zonder reden.  
 • De taal is dwergeng of wil je nieuwsgierig maken.  
 • Bevatton soms taalfouten of zijn vreemd geschreven.  
 • Een vage aanspreektel of je e-mailadres als aanspreking.  
 • Een onbekende afzender of foute e-mailadressen.

De belangrijkste tip!  
 Bevat het bericht een link? Klik niet zomaar! zweef met je muis over de link zonder te klikken. Nu

## Les matériels de campagne, à la disposition des services de police



## Campagne 2020 : Les mots de passe c'est dépassé

---



## Campagne 2021 : Déjouez le phishing



**Wees slimmer  
dan een phisher**

**Altijd actuele info op zak  
met de Safeonweb app**

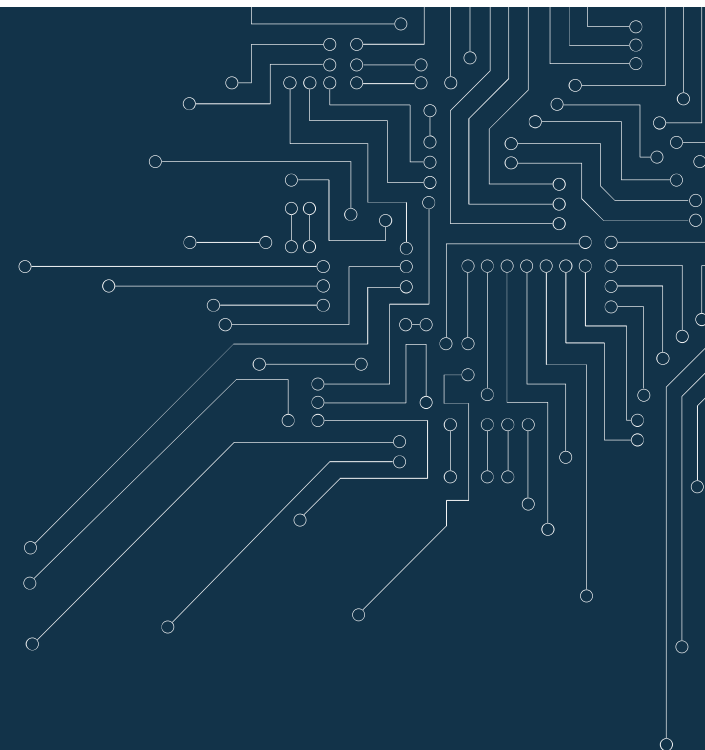


**Soyez malin.  
Déjouez le phishing.**

**Toujours des infos actualisées  
dans la poche avec  
l'application Safeonweb**

# 2.

## Phishing



## Qu'est-ce que le phishing ?

---





ING

---

Vanwege een of meerdere ongebruikelijke inlogpogin(en) is uw rekening tijdelijk beperkt. Verifieer uw account nu: [ingbe-service.info](https://ingbe-service.info)

## Verificatie van uw account!

Geachte relatie,

We hebben inwendig onderzoek gedaan naar uw KBC account en uit onderzoek is gebleken dat u niet voldoet aan de algemene voorwaarden. Uit voorzorgsmaatregelen willen wij dat u een verificatie verricht voor het controleren van uw KBC account. Verricht u deze procedure niet dan zijn wij genoodzaakt uw KBC rekening te schorsen.

[kbc-mijnformulier.info](https://kbc-mijnformulier.info)

Mocht u niet in de gelegenheid zijn om de verificatie binnen 24 uur te voltooien, dan kunt u uw account ook opnieuw activeren door met uw betaalpas en een geldig legitimatiebewijs langs te gaan bij een KBC kantoor naar keuze.

Met vriendelijke groet,

KBC Belgium Groep

[Belasting] Op 1-12-2020 heeft de overheid besloten om elk huishouden een bedrag van €202,68 toe te kennen ter compensatie van uw water- en energiefactuur. Klik hier om uw compensatie te ontvangen : <https://s.id/fod-belasting>

[FOD]

Uw openstaande schuld met kenmerk BD29382736483 is, na meerdere herinneringen, niet voldaan. Op 11 november 2020 zal de gerechtsdeurwaarder overgaan tot conservatoir beslag. U kunt de beslagprocedure voorkomen door direct het bedrag van €7,32 te voldoen via: <https://bit.ly/incassobureauFOD>

## Les messages de phishing surfent sur l'actualité : COVID-19

---



# Prévention

The screenshot shows the Safeonweb.be website with a green background. At the top, there are navigation links: 'ACTUALITÉ', 'BLOG', 'CONSEILS', 'MATÉRIEL DE CAMPAGNE', 'LIENS', and 'CONTACT'. The main heading is 'FAITES LE Test du phishing'. Below it, a question asks 'Identifiez-vous à temps les messages suspects?'. Two columns of text provide information: the left column asks 'Savez-vous à quoi vous devez être attentif(ve) en cas de messages suspects?' and the right column asks 'Vous n'avez pas le temps de faire le test?'. A third section asks 'Vous avez reçu un message suspect?'. At the bottom, there is an image of a group of people holding a check for €250 and a document. Logos for the Centre for Cyber Security Belgium and the Cyber Security Coalition are visible.

NL FR EN      Autres informations et services du gouvernement: www.belgium.be .be

Safeonweb.be      ACTUALITÉ BLOG CONSEILS MATÉRIEL DE CAMPAGNE LIENS CONTACT

## FAITES LE Test du phishing

**Identifiez-vous à temps les messages suspects ?**

**Savez-vous à quoi vous devez être attentif(ve) en cas de messages suspects ?**

Dans le cadre du test du phishing, nous vérifions si vous faites preuve d'assez de vigilance pour repérer les messages suspects. Êtes-vous déjà passé(e) maître dans l'art d'identifier les messages suspects ? Ou avez-vous encore besoin d'un peu d'entraînement ?

**Faites le test**

**Vous n'avez pas le temps de faire le test ?**

Découvrez ici nos astuces pour identifier les tentatives de phishing

**Découvrez nos conseils ici**

**Vous avez reçu un message suspect ?**

Envoyez-le à l'adresse [suspect@safeonweb.be](mailto:suspect@safeonweb.be) et supprimez-le ensuite.

Si vous recevez ce message au travail, vous devez suivre les procédures en vigueur pour le phishing. Par exemple, l'envoyer vers le service ICT.

**Qu'est-ce que [suspect@safeonweb.be](mailto:suspect@safeonweb.be) ?**

**CHEQUE €250**

CENTRE FOR CYBER SECURITY BELGIUM      .be

CYBER SECURITY COALITION      Safeonweb.be

# Prévention



# Prévention

---



## Prévention

---



## Prévention : reconnaissez le phishing à temps

---

- Le message est-il inattendu ?
- Le message est-il urgent ?
- Où mène le lien sur lequel on vous incite à cliquer ?

## Conseil : Transférez les messages suspects

Transférez les messages suspect vers [suspect@safeonweb.be](mailto:suspect@safeonweb.be). Des captures d'écran de messages suspect peuvent également être transmises.

Quel sort réservons-nous aux mails ?



1. Analyse des URL
2. Signalé comme phishing
3. Envoi à Google Safe Browsing + Microsoft Smartscreen
4. Avertissement dans le navigateur



## Questions fréquemment posées sur [suspect@safeonweb.be](mailto:suspect@safeonweb.be)

---

- Je transfère de nombreux mails à [suspect@safeonweb.be](mailto:suspect@safeonweb.be) mais je continue de recevoir des messages de phishing. Comment est-ce possible ?
- Je ne parviens pas à transférer des messages suspects à [suspect@safeonweb.be](mailto:suspect@safeonweb.be). Comment est-ce possible ?
- Je reçois parfois un message m'indiquant que mon message ne peut pas être envoyé à [suspect@safeonweb.be](mailto:suspect@safeonweb.be). Que se passe-t-il ?
- Quand dois-je transférer des messages ?
- Est-ce que je recevrai un message après avoir transféré un message suspect à [suspect@safeonweb.be](mailto:suspect@safeonweb.be) ?
- Safeonweb lit-il tous les mails ?
- Que dois-je faire si je me pose des questions sur la cybersécurité ?

## Résultats 2020 suspect@safeonweb.be

---

- Total des mails reçus : 4.575.000 ( $\approx$  12.000/jour)
- Total des URL uniques bloquées pour cause de phishing : 1.433.000 ( $\approx$  4.000/jour)

## Informations pour les victimes

---

- Si vous avez communiqué un mot de passe que vous utilisez pour d'autres sites, modifiez-le immédiatement.
- Utilisez l'authentification à deux facteurs
- Déposez plainte à la police si vous êtes victime
- Si vous avez communiqué vos données bancaires ou de Itsme, prévenez immédiatement votre banque et Cardstop
- Transmettez le message à [suspect@safeonweb.be](mailto:suspect@safeonweb.be)

# 3.

## Arnaque/fraude en ligne

## Qu'est-ce que l'arnaque/la fraude en ligne ?



Source : SPF Économie

## Exemples

---

1. Fausses boutiques en ligne
2. Fraude aux comptes à sécurité renforcée
3. Fraude à l'amitié
4. Bitcoin scam
5. Microsoft scam
6. Fraude au CEO
7. Sextorsion scam

## Focus case : MICROSOFT SCAM

---



## Prévention

---

- Méfiez-vous toujours des appels téléphoniques de sociétés qui vous demandent de réaliser une série d'actions sur votre ordinateur.
- Ne laissez pas une personne que vous ne connaissez pas prendre le contrôle de votre ordinateur.
- N'effectuez pas de paiement, même de quelques euros, si une personne inconnue a pris le contrôle de votre ordinateur





## Information à destination des victimes

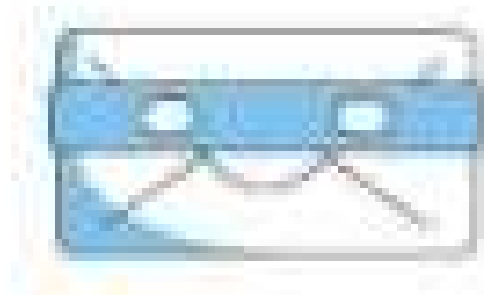
---

- Si vous êtes victime, déposez plainte à la police
- Si vous avez communiqué vos données bancaires, prévenez immédiatement votre banque et Cardstop
- Signalez la fraude (Internet) sur :  
<https://pointdecontact.belgique.be>

## Focus case : FRAUDE AU CEO

---

URGENT



FLOU

## Prévention

---

- Les entreprises peuvent s'armer contre la fraude au CEO en informant correctement leurs collaborateurs et en les mettant en garde contre ce type de pratique
- Des procédures étanches pour les paiements sont indispensables

## Informations pour les victimes

---

- Si vous êtes victime, portez plainte à la police
- Si vous avez transmis des données, prenez contact avec votre banque et Cardstop
- Signalez la fraude (sur Internet) sur la page :  
<https://pointdecontact.belgique.be/meldpunt/fr/bienvenue>

## Focus case : SEXTORTION SCAM ou arnaque par sextorsion

<-> sextorsion (= extorsion sexuelle)

### Arnaque

= faire croire à la victime que son ordinateur a été piraté et qu'on a accès à sa caméra

- Ancien mot de passe trouvé sur Internet.  
<https://haveibeenpwned.com/>
- *Spoofing* de votre adresse e-mail.  
Réception d'un message qui semble venir de votre propre adresse e-mail.

-----Oorspronkelijk bericht-----

Van:

Verzonden: woensdag 6 februari 2019 19:48

Aan:

Onderwerp: Zorg ervoor dit bericht te lezen! Uw persoonlijke gegevens worden bedreigd!

Hallo!

Zoals je misschien hebt gemerkt, heb ik je een e-mail van je account gestuurd.  
Dit betekent dat ik volledige toegang tot uw account heb.

Ik hou je nu al een paar maanden in de gaten.  
Het is een feit dat je bent geïnfecteerd met malware via een site voor volwassenen die je hebt bezocht.

Als je hier niet bekend mee bent, zal ik het uitleggen.  
Trojan Virus geeft me volledige toegang tot en controle over een computer of ander apparaat.  
Dit betekent dat ik alles op je scherm kan zien, de camera en microfoon kan inschakelen, maar je verdenkt het niet.

Ik heb ook toegang tot al uw contacten en al uw correspondentie.

Waarom heeft uw antivirus geen malware gedetecteerd?

Antwoord: Mijn malware gebruikt de driver, ik update zijn signatures elke 4 uur zodat uw antivirus stil is.

Ik heb een video gemaakt die laat zien hoe jij bevreemdt jezelf stelt in de linkerhelft van het scherm (je begrijpt zeker wat ik bedoel ...), en in de rechterhelft zie je de video die je hebt bekeken.  
Met een muis klik kan ik deze video verzenden naar al uw e-mails en contacten op sociale netwerken.  
Ik kan ook de toegang posten tot al uw e-mailcorrespondentie en messengers die u gebruikt.

Als je dit wilt voorkomen,  
breng het bedrag van 358 EURO over naar mijn bitcoin-adres (als je niet weet hoe je dit moet doen, schrijf dan naar Google: "Koop Bitcoin").

Mijn bitcoin-adres (BTC Wallet): 12PUa25HjWAUEpZZUxQNvxa7epab7g2Ksb

Na ontvangst van de betaling, zal ik de video verwijderen en je zult me nooit meer horen.  
Ik geef je 48 uur om te betalen.

Zodra u deze e-mail opent, werkt de timer. Ik ontvang onmiddellijk een melding over dit evenement.

Onthouden, na de tijd die aan u is gegeven, wordt de video onmiddellijk verspreid!

Het heeft geen zin om te klagen bij de politie, omdat deze brief niet kan worden getraceerd als en mijn bitcoin-adres.  
Ik maak geen fouten.

Als ik zie dat je dit bericht met iemand anders hebt gedeeld, wordt de video onmiddellijk verspreid.

Beste wensen!

## Focus case : SEXTORTION SCAM ou arnaque par sextorsion

Exemple de 2021:

- Nous recevons de nombreux rapports de faux messages qui semblent provenir de la police fédérale et d'Europol.
- La victime est prétendument convoqué dans le cadre d'infractions sexuelles.
- Le message apparaît comme très sérieux et coercitif.
- L'intention est d'effrayer et d'extorquer de l'argent.
- Ce type d'escroquerie n'est pas nouveau, mais il continue de circuler et d'effrayer beaucoup de gens.



À votre attention,  
À la demande de Madame, Catherine DE BOLLE commissaire générale de la police fédérale, élue au poste de directrice d'Europol " Brigade de protection des mineurs (BPM) " nous vous adressons cette convocation.

La COPJ ou convocation par officier de police judiciaire est prévue par l'article 390-1 du Code de Procédure Pénale. Elle vaut citation devant le Tribunal et est décidée par le Procureur de la République.

En application des dispositions de l'article 372 du code pénal énonce : " Tout attentat à la pudeur commis sans violences ni menaces sur la personne ou à l'aide de la personne d'un enfant de l'un ou de l'autre sexe, âgé de moins de seize ans accomplis, sera puni de la réclusion.

L'article 227-23 du Code pénal dispose : « Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende.

Nous engageons à votre rencontre, des poursuites judiciaires peu après une saisie informatique de la Cyber-infiltration pour :

- Pédopornographie
- Pédophilie
- Exhibitionnisme
- Cyber pornographie
- Trafic sexuel

Pour votre information, la loi de mars 2007 aggrave les peines lorsque les propositions, les agressions sexuelles ou les viols ont pu être commis en recourant à internet et vous avez commis les infractions après avoir été ciblé sur internet (site d'annonce), puis pendant des échanges mails.  
Les photos/vidéos dénudées de vous que vous envoyez aux mineurs ont été enregistrées par notre cyber gendarme et constituent les preuves de vos infractions.

Cette convocation présente un caractère obligatoire. Conformément à l'article 78 du code pénal, l'officier de police judiciaire peut contraindre à comparaître par la force publique, avec l'autorisation préalable du procureur de la République, les personnes qui n'ont pas répondu à une convocation à comparaître ou dont on peut craindre qu'elles ne répondent pas à une telle convocation.

Dans un souci de confidentialité nous vous adressons cet e-mail, vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications pour qu'elles soient mises en examen et vérifiées afin d'évaluer les sanctions, cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport à Mme Myriam Quémener, procureur adjoint au tribunal de grande instance de Créteil et spécialiste de cybercriminalité pour établir un mandat d'arrêt à votre rencontre, nous vous adresserons dans ce cas une lettre recommandée avec accusé de réception ( arrestation immédiate ) par la gendarmerie la plus proche de votre «Lieu de résidence » et vous serez fiché au registre national des délinquants sexuels. Dans ce cas, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux medias pour publication de personne fiché au RND.

\*En cas de non-respect de la procédure et du délai, la lettre de convocation vous sera envoyée par courrier postal.  
Cordialement,

Mme Catherine De Bolle, commissaire générale de la police fédérale, élue au poste de directrice d'Europol" la brigade de protection des mineurs (BPM)"

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE  
BRIGADE DE PROTECTION DES MINEURS  
Adresse : RUE ROYALE 202 A, 1000 Bruxelles, Belgique  
24H/24H  
DETACHEMENT DU DEPARTEMENT DE LA PREFECTURE DE POLICE DE PARIS (BPM)  
36 RUE DU BASTION, 75017 PARIS



## Prévention

---

- Ne cédez pas aux demandes d'argent
- Supprimez le message
- Marquez le message comme spam ou indésirable
- Bloquez l'expéditeur

## Informations pour les victimes

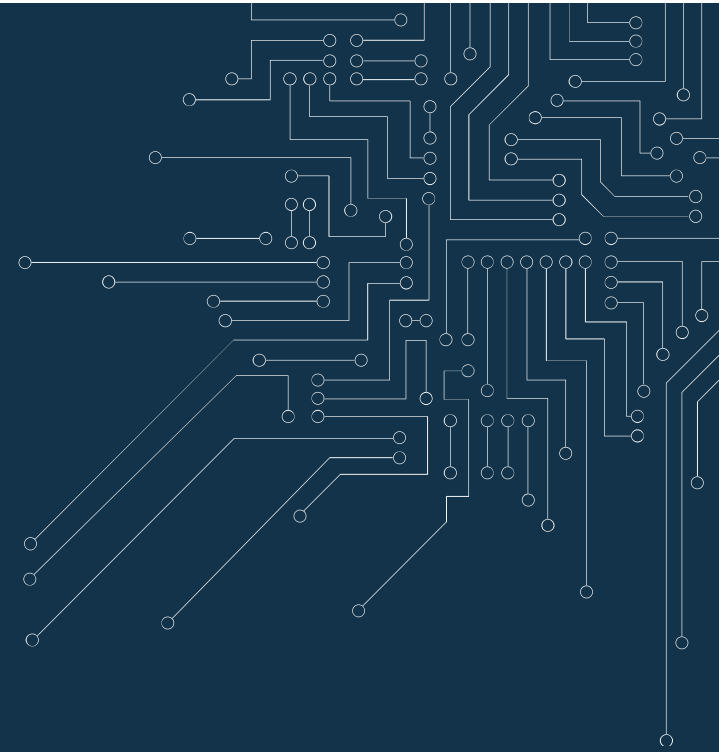
---

- Si vous êtes victime, portez plainte à la police
- Conservez un maximum d'éléments de preuve (e-mails, messages, captures d'écran...)
- Si vous avez transmis des données, prenez contact avec votre banque et Cardstop
- Signalez la fraude (sur Internet) sur la page :  
<https://pointdecontact.belgique.be/meldpunt/fr/bienvenue>



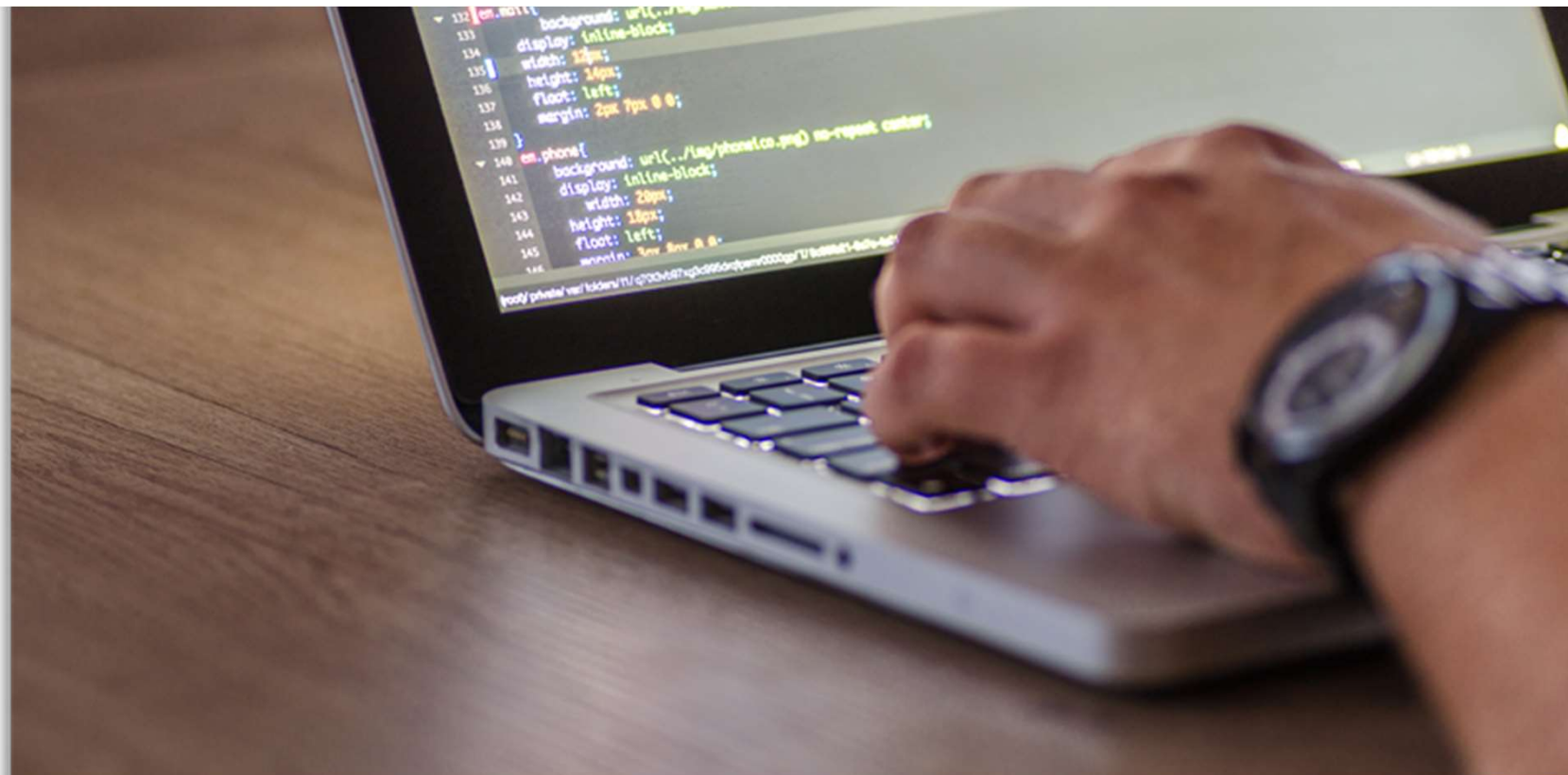
# 4.

## Malware



## Qu'est-ce qu'un malware?

---



## Exemples

---

Formes de malware:

- Virus
- Trojan
- Worm
- Ransomware
- Spyware
- Rootkit
- Keylogger
- Backdoor
- Etc.

# Prévention

---



## Focus case : RANSOMWARE

---



## Prévention

---

- Procédez systématiquement aux mises à jour de vos appareils et applications
- Utilisez un scanner antivirus
- Effectuez régulièrement des copies de sauvegarde (back-ups) pour pouvoir récupérer vos données en cas de perte

Si vous êtes victime d'un ransomware, évitez un maximum de dégâts :

- Désactivez le Wi-Fi ou retirez le câble Internet.
  - Débranchez immédiatement tous les autres appareils, comme un disque dur externe ou une clé USB.
-

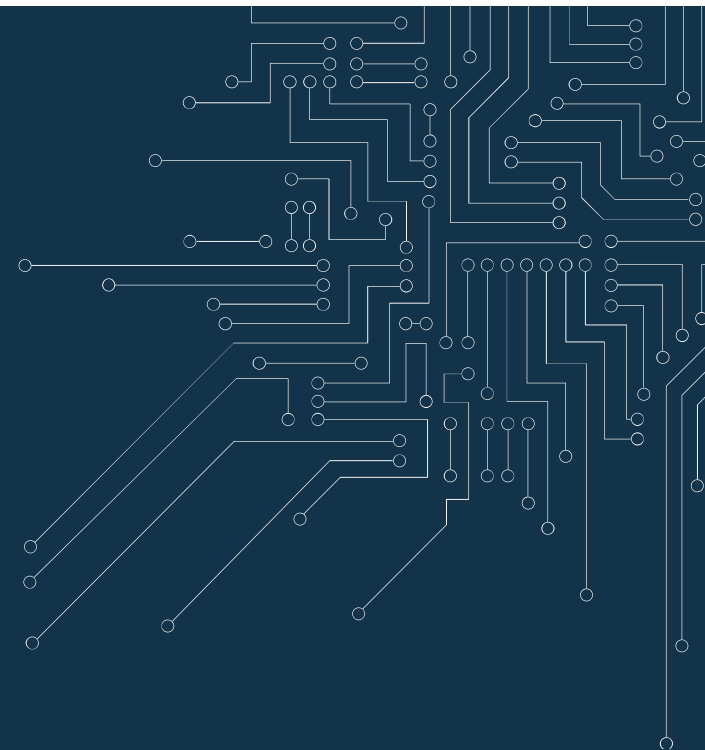
## Informations pour les victimes

---

- Ne payez pas : vous n'aurez aucune garantie de réellement récupérer vos données de manière sécurisée. De plus, le risque que le virus n'ait pas été entièrement supprimé ou qu'il cache un moyen dérobé d'infecter à nouveau votre appareil à l'avenir reste réel.
  - Allez voir sur [www.nomoreransom.org](http://www.nomoreransom.org) si la clé est disponible pour ce ransomware.
  - Déposez plainte à la police
  - Conservez un maximum d'éléments de preuve (e-mails, captures d'écran...) et présentez-les à la police
  - Prenez contact avec CERT.be pour signaler l'incident et éventuellement demander de l'aide : <https://www.cert.be/fr/signaler-un-incident>
  - Signalez la fraude (sur Internet) sur la page : <https://pointdecontact.belgique.be/meldpunt/fr/bienvenue>
-

# 5.

## Piratage de compte





## Qu'est-ce qu'un account hack?

---

**Plusieurs comptes** peuvent faire l'objet d'un piratage : réseaux sociaux, e-mail, banque, boutiques en ligne, etc.

Le compte peut être piraté **de différentes manières** : en obtenant les identifiants de connexion par le phishing, par une attaque de force brute (c'est-à-dire en « devinant » les mots de passe), etc.



## Exemple : Instagram, Office 365, ou autre piratage de compte

**From:** Microsoft office365 Team [<mailto:cyh11241@lausd.net>]  
**Sent:** Monday, September 25, 2017 1:39 PM  
**To:**  
**Subject:** Your Mailbox Will [Shutdown](#) Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please [verify](#).

[Verify Now](#)

Microsoft Security Assistant  
Microsoft office365 Team! ©2017 All Rights Reserved



### Copyright Infringement

Hi  
We regret to inform you that your account will be suspending because you have violated thecopyright laws. Your account will be deleted within 24 hours. If you think we make a mistake please verify, to secure your account.

[Secure My Account](#)

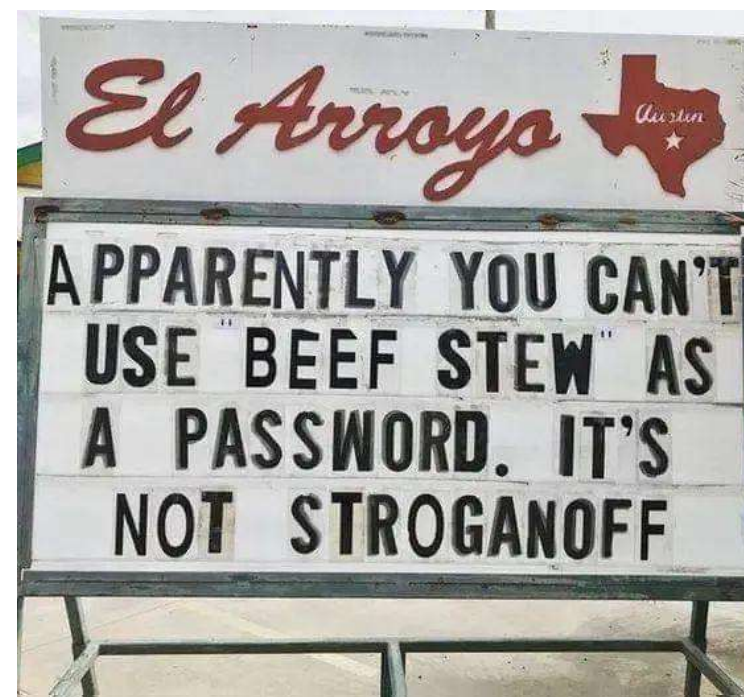
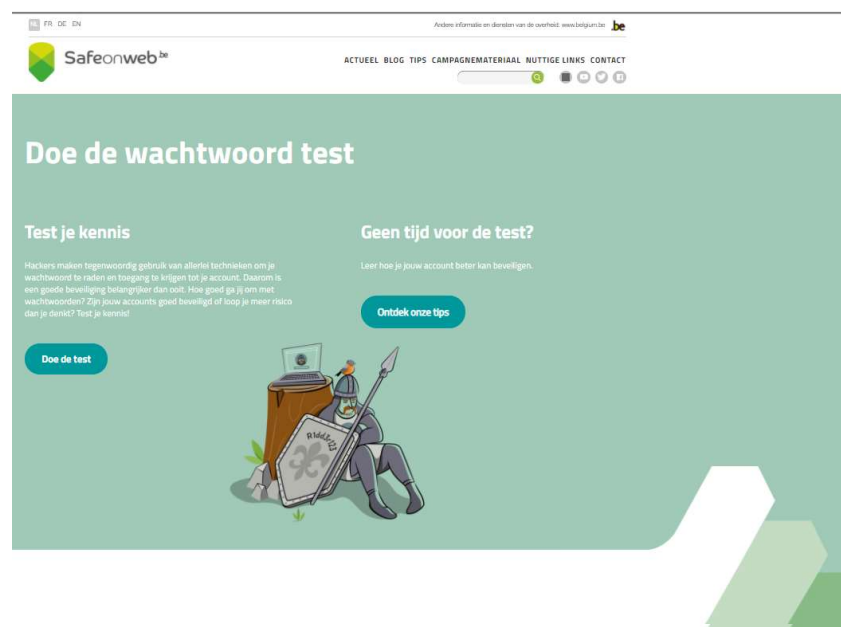
## Conseils : piratage d'un compte

---

- Modifiez immédiatement votre mot de passe
  - (sur tous les autres comptes où vous utilisez ce mot de passe)
- Prévenez vos contacts
- Activez l'authentification à deux facteurs
- Si vous ne pouvez plus accéder à votre compte :
  - informez la plateforme pour qu'elle rétablisse votre compte

## Prévention

Votre mot de passe est-il suffisamment sûr ? Faites le test : <https://safeonweb.be/fr/test-du-mot-de-passe>



## Prévention

---

Un gestionnaire de mots de passe

- permet de mettre en lieu sûr tous vos comptes et mots de passe.
- vous aide à créer des mots de passe sûrs. Il vous suffit d'indiquer le nombre et le type de caractères que vous souhaitez utiliser et votre gestionnaire de mots de passe sécurisé vous propose un mot de passe complètement aléatoire.
- est lui-même sécurisé par un mot de passe sûr. Il vous suffit donc de vous souvenir d'un seul mot de passe sûr.

Multi-Factor Authentication (MFA)

- avec quelque chose que vous seul connaissez (votre mot de passe ou votre code PIN),
- avec quelque chose que vous seul avez (votre téléphone ou votre token),
- avec quelque chose que vous êtes (votre empreinte digitale, votre visage, votre iris...).



# Prévention

---



## Focus case : piratage IoT

---

- Frigos, réveils, voitures, machines à café, systèmes de chauffage, alarmes, jouets... de plus en plus d'appareils sont connectés. Internet devient ainsi un « Internet des objets », un « Internet of Things ».
- Connecter des appareils à Internet n'est jamais dénué de risques.



# Exemple INSECAM.org



Watch Axis camera in Belgium,Brussels



Watch Defeway camera in Belgium,Brussels



Watch PanasonicHD camera in Belgium,Brussels



Watch Axis camera in Belgium,Brussels



Watch Foscam camera in Belgium,Brussels



Watch Defeway camera in Belgium,Brussels



Watch Axis camera in Belgium,Brussels



Watch Defeway camera in Belgium,Brussels



Watch PanasonicHD camera in Belgium,Brussels



Watch Axis camera in Belgium,Brussels



Watch Foscam camera in Belgium,Brussels



Watch Defeway camera in Belgium,Brussels



## Prévention

---

- Lisez attentivement les conditions d'utilisation des données à caractère personnel et adaptez au besoin les paramètres en la matière.
- Autorisez uniquement votre appareil à accéder à des données qui sont strictement indispensables.
- Remplacez toujours les mots de passe installés par défaut, par de nouveaux mots de passe sûrs.
- Sécurisez votre réseau privé à l'aide d'un mot de passe fort.
- Installez toujours les mises à jour de vos appareils dès qu'elles sont disponibles.
- Éteignez vos appareils quand vous ne les utilisez pas.

## Informations pour les victimes

---

- Déposez plainte à la police
- Conservez un maximum d'éléments de preuve (e-mails, messages, captures d'écran...) et présentez-les à la police
- Signalez la fraude (sur Internet) sur la page :  
<https://pointdecontact.belgique.be/meldpunt/fr/bienvenue>



CENTRE FOR  
CYBER SECURITY  
BELGIUM

# Tenez-vous au courant des escroqueries actuelles par le biais de l'application Safeonweb

---



## 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.

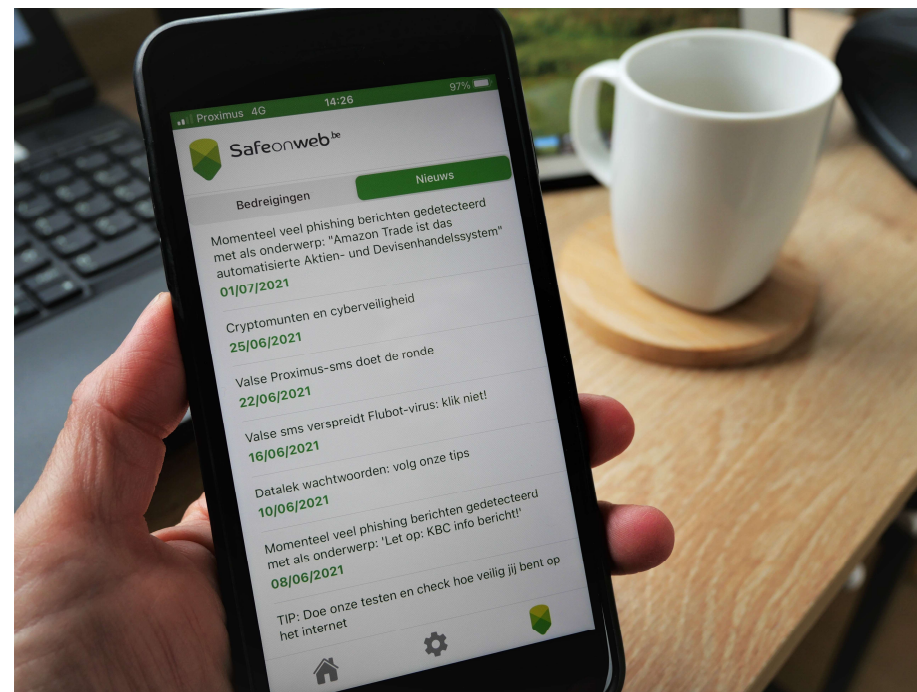
[Plus d'information >](#)



## Pourquoi?

Un moyen rapide et facile de se tenir au courant des tentatives d'escroquerie actuelles

Pour recevoir une alerte en cas de problème sur votre réseau domestique



## Teaser video

---



## To Card Stop or not to Card Stop?

---

Les victimes doivent contacter Card Stop en cas de

- vol
- Perte
- l'utilisation frauduleuse de leur carte de débit ou de crédit

Card Stop bloque les cartes de paiement. Mais il est également important de contacter la banque de la victime.



## Contactez Card Stop et la banque

- si la victime est toujours en possession de la carte mais ne reconnaît pas certaines opérations sur les relevés de compte
- ou s'il/elle a donné son code PIN ou son code de réponse personnel à un escroc

Via: <https://cardstop.be/fr/home/Je-veux-bloquer/Bloquez-via-lemetteur.html>

Via: <https://macarte.be/fr/home.html>



JE VEUX BLOQUER UN MOYEN DE PAIEMENT J'AI BLOQUÉ UN MOYEN DE PAIEMENT

Faire bloquer l'accès à votre application bancaire par le biais de votre banque

### Faire bloquer l'accès à votre application bancaire par le biais de votre banque

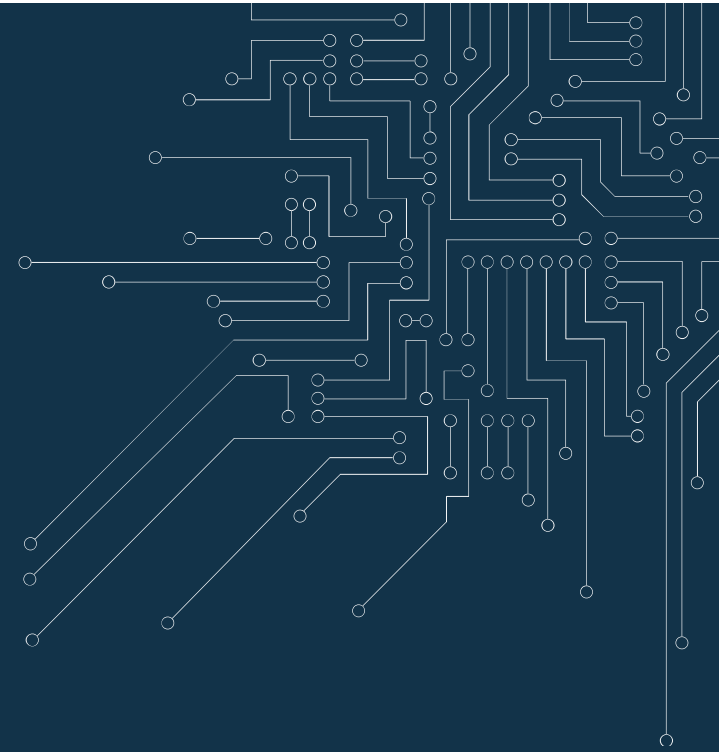
Un soupçon de fraude ou d'abus de votre application bancaire ? Contactez immédiatement votre banque.

Nous vous conseillons également à titre préventif, de faire bloquer vos applications de paiement en cas de perte, de vol ou de revente de votre appareil mobile (smartphone, tablette, montre intelligente, appareils connectés).

Argenta  
Axa  
Banque Van Breda  
Belfius  
Beobank  
BNP Paribas Fortis  
bpost bank  
CBC  
CPH  
Crelan  
Deutsche Bank  
Europabank  
Fintro  
Hello Bank  
ING  
KBC

# 6.

## Conclusion

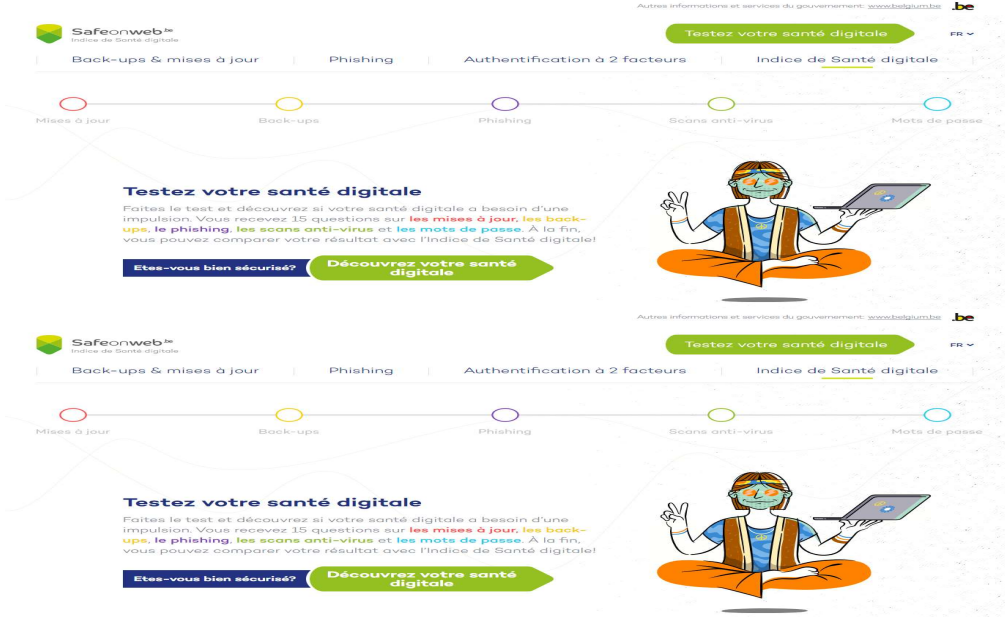




# Testez votre santé digitale !

Êtes-vous en bonne santé digitale ?

Faites le test :



## Suivez-nous :

---

[www.safeonweb.be](http://www.safeonweb.be)

[www.cert.be](http://www.cert.be)

[www.ccb.belgium.be](http://www.ccb.belgium.be)

### Suivez-nous sur Facebook:

<https://www.facebook.com/Safeonweb.be/>

### Suivez-nous sur Twitter:

[https://twitter.com/safeonweb\\_be](https://twitter.com/safeonweb_be)

<https://twitter.com/certbe>

### Suivez-nous sur YouTube: Safeonweb.be

### Suivez-nous sur LinkedIn:

<https://www.linkedin.com/company/centre-for-cybersecurity-belgium>

---

## Utilisation de cette présentation

---

- Cette présentation est destinée aux professeurs qui souhaitent présenter le CCB et ses services et qui souhaitent donner un aperçu des différentes cyberattaques
- Le groupe cible : les adultes, peut éventuellement être adaptée à un public plus jeune
- La présentation (en tout ou partie) peut être utilisée librement à condition de mentionner la source et uniquement à des fins non commerciales

## Contact

---

### Centre pour la Cybersécurité Belgique

Rue de la Loi 16

1000 Bruxelles

[info@ccb.belgium.be](mailto:info@ccb.belgium.be)

## Disclaimer

---

Le CCB met tout en œuvre pour assurer au mieux l'actualisation, l'accessibilité, l'exactitude et l'exhaustivité du contenu et des mises à jour publiés sur ce site. En cas de modification, une nouvelle version sera publiée le cas échéant.

La présente note contient des liens vers des sites publiés par des tiers et qui ne relèvent pas de la gestion du CCB. Ces informations sont également susceptibles de changer à tout moment.

Le CCB ne peut être tenu responsable de tout dommage causé par l'utilisation de ces informations. En outre, aucun droit ne peut dériver des informations fournies par des tiers.