Safeonweb.be

LES ESCROQUERIES EN LIGNE : COMMENT LES REPÉRER, LES PRÉVENIR ET RÉAGIR ?

Pour plus d'infos et d'autres formes d'escroqueries, rendez-vous sur safeonweb.be/fr

CENTRE FOR CYBERSECURITY BELGIUM

.be

Phishing

Le phishing est une escroquerie en ligne à l'aide de faux mails, sites Internet, SMS, QR code … L'objectif étant de collecter vos informations personnelles.

- Réfléchissez avant de cliquer, les offres peuvent être trompeuses.
- Ne donnez jamais de mots de passe, de codes de cartes bancaires ou de codes de réponse du digipass par mail, appel téléphonique, SMS ou médias sociaux.
- Vérifiez l'adresse de l'expéditeur et l'URL des liens vers lesquels on vous envoie.
- Apprenez à reconnaître les messages suspects sur surfersanssoucis.safeonweb.be.

Fraude à l'investissement

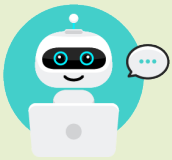
Vous êtes contacté par téléphone ou par mail (ou via le compte piraté d'un ami) par une soi-disant société d'investissement qui vous propose d'acheter des actions ou d'autres produits financiers. Il peut également s'agir d'une fausse publicité dans laquelle une célébrité vante ces investissements.

- Méfiez-vous des propositions financières que vous n'avez pas sollicitées et montrez-vous critique à l'égard des offres.
- Vérifiez l'identité du prestataire même s'il semble s'agir d'une société autorisée : nom, siège social, coordonnées.

Problème de PC (Tech Scam)

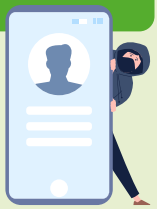
- Méfiez-vous des appels téléphoniques provenant de sociétés qui vous demandent d'effectuer une série d'actions sur votre ordinateur.

> Je suis Marc du helpdesk de Microsoft. Votre ordinateur rencontre un problème de sécurité. Je vais prendre les commandes de votre ordinateur pour vous aider.



- Si un pop-up apparaît pour signaler que votre ordinateur est bloqué, ne contactez pas le numéro indiqué. Effectuez un scan antivirus.
- N'installez jamais d'application ou de logiciel proposé par le soi-disant helpdesk. Il pourrait alors prendre le contrôle de votre appareil.

Usurpation d'identité/compte piraté



> « Il se passe des choses étranges sur mon compte : j'ai soi-disant envoyé des messages à mes amis sans le savoir, des messages et des photos apparaissent sur ma page alors que je n'ai rien publié. »

Votre compte est probablement la cible d'un pirate qui en a forcé l'accès.

- Vous avez encore accès à votre compte ? Modifiez alors immédiatement le mot de passe de ce compte et de tous vos autres comptes et prévenez vos contacts.
- Vous n'avez plus accès à votre compte ? Utilisez les options de récupération du compte (option 'mot de passe oublié') pour retrouver l'accès et modifiez ensuite tous vos mots de passe.
- Activez l'authentification à deux facteurs. Lors de la première étape, vous vous connectez à votre compte à l'aide de votre mot de passe. A la deuxième étape, ce compte envoie un code à votre téléphone portable que vous introduisez pour accéder à votre compte.
- Utilisez pour chaque compte un mot de passe (fort) différent et conservez-les dans un gestionnaire de mots de passe. Il s'agit d'un coffre-fort en ligne rassemblant vos mots de passe par compte et sécurisé lui-même par un mot de passe.

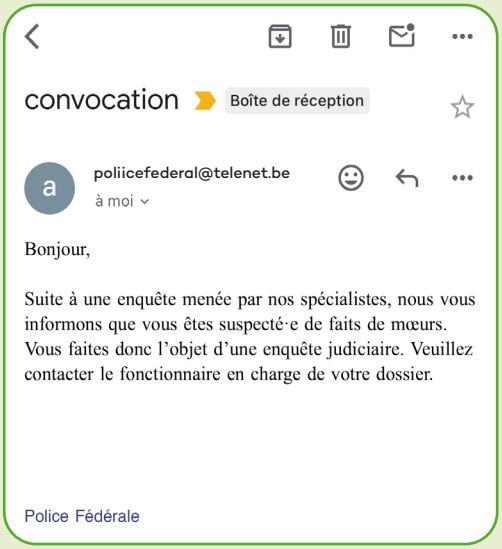
Arnaque sur site de vente en ligne

Arnaque qui vise l'acheteur ou le vendeur sur des sites de ventes en ligne. Il peut s'agir de faux vendeurs, faux acheteurs ou encore faux sites web.

> Bonjour, cet article est-il toujours disponible ? Je vous offre 500 € pour votre table. Je ne peux pas venir la chercher donc un chauffeur DPD viendra l'enlever. Je vous payerai par virement bancaire.

- Méfiez-vous des réponses trop rapides et des offres supérieures au prix demandé. Vérifiez le profil de l'acheteur/vendeur.
- Poursuivez toujours vos conversations avec les acheteurs/vendeurs sur le site de vente en ligne et non par SMS ou sur WhatsApp par exemple.
- Ne payez jamais via un lien qui vous est envoyé par un acheteur ou un vendeur. Ces liens vous conduisent à un faux site web où les fraudeurs vous demandent vos coordonnées bancaires.
- N'encodez jamais vos informations personnelles sur un site de transport via un lien fourni par l'acheteur/le vendeur.

Message semblant provenir de la police



Arnaque via mail misant sur l'urgence et la gravité des faits reprochés.

- Ne réagissez jamais à un message de ce type et ne cédez pas aux demandes d'argent.
- Bloquez l'expéditeur.
- Contactez l'organisme émetteur via les coordonnées que vous avez vous-même recherchées.

Ma check-list de sécurité en ligne

- ✅ Je ne donne jamais de mots de passe, de codes de carte bancaire ou de codes de réponse par mail, appel téléphonique, SMS ou médias sociaux.
- ✅ Je protège ma boîte mail et mes comptes de réseaux sociaux avec l'authentification à deux facteurs.
- ✅ J'installe les mises à jour dès qu'elles apparaissent.
- ✅ J'installe un antivirus sur mon ordinateur, si je n'en ai pas déjà un.
- ✅ Je fais des sauvegardes de mes fichiers sur le cloud ou un disque dur externe.

Trop tard, vous êtes victime. Que faire ?

Vous avez transmis vos données bancaires, vous constatez des retraits d'argent frauduleux sur votre compte, vous avez transféré de l'argent à un escroc ?

- Contactez le service Card Stop au 078 170 170 afin de bloquer l'accès à vos comptes.
- Contactez votre banque. Plus vous l'avertissez rapidement, plus vous augmentez vos chances de récupérer l'argent.
- Déposez plainte auprès de la police locale. Munissez-vous d'un maximum d'informations : extraits de compte, capture d'écran du message ou du site web frauduleux, profil et conversations avec le suspect, application installée, …

LES OUTILS POUR VOUS PROTÉGER

VOUS AVEZ REÇU UN MAIL OU UN MESSAGE SUSPECT ?

Envoyez-le à l'adresse suspect@safeonweb.be et supprimez-le ensuite. Les annexes et liens suspects seront analysés (processus automatisé). Lorsqu'un internaute moins attentif clique sur ce lien, il reçoit un avertissement clair l'invitant à ne pas se rendre sur cette page.

INSTALLEZ L'EXTENSION DE NAVIGATEUR SAFEONWEB

L'extension de navigateur Safeonweb vous avertit lorsque vous visitez un site web non sécurisé et qu'il est dangereux de saisir vos données. Un code couleur (visible dans la barre d'outils) vous indique si le site web est fiable ou non. Regardez comment l'installer sur safeonweb.be.

REGARDEZ NOTRE SÉRIE D'E-LEARNING SURFER SANS SOUCI

Apprenez à détecter les arnaques et les messages suspects en regardant notre série d'e-learning sur surfersanssoucis.safeonweb.be.

TÉLÉCHARGEZ L'APPLICATION SAFEONWEB

L'application Safeonweb vous informe sur les menaces qui planent actuellement sur le pays et vous prodigue des conseils pour améliorer votre sécurité en ligne.
Elle est disponible gratuitement pour iOS dans l'App Store et pour Android dans le Google Play Store.

PLUS D'INFOS ?

- **safeonweb.be/fr**
- **surfersanssoucis.safeonweb.be/fr/modules**

Suivez Safeonweb