QUE FAIRE SI VOUS AVEZ ETE VICTIME?

Si vous avez communiqué vos coordonnées bancaires, prévenez le plus rapidement possible votre banque afin de bloquer la ou les transaction(s) frauduleuse(s).

Vous pouvez également le faire via Card Stop.

DÉPOSEZ PLAINTE LE PLUS RAPIDEMENT POSSIBLE

EN VEILLANT À AVOIR LES INFORMATIONS SUIVANTES:

- Vous avez communiqué vos coordonnées bancaires ? Prenez le numéro de référence de Card Stop et l'adresse URL complète du site frauduleux (en cliquant dessus 1 fois).
- L'argent a disparu de votre compte en banque ? Prenez les extraits de compte avec date et heure des retraits. Emportez votre numéro de compte et numéro de carte bancaire.
- Vous avez eu des contacts avec quelqu'un sur les réseaux sociaux ? Faites une capture d'écran du profil du suspect et des discussions que vous avez eues.
- Vous avez ouvert un faux site Internet qui ressemblait par exemple à celui de votre banque ou d'une autre institution ? Faites une capture d'écran et emportez-la.
- Vous avez été escroqué par un site de vente en ligne ? Faites une capture d'écran de l'annonce ou de l'offre à laquelle vous avez réagi et du profil de l'escroc.
- Vous avez reçu un mail de l'escroc ? Conservez-le et imprimez-le avec en-tête complète.

CONTACTS UTILES

Pour savoir si un site peut être consulté en toute sécurité, consultez d'abord l'état de sécurité à gauche de l'adresse Web (URL):

- Sécurisé (« https »)
- Informations ou Non sécurisé
- Non sécurisé ou Dangereux

JOIN NOW

Même si vous voyez le sigle « https », faites toujours preuve de prudence et vérifiez si vous êtes bien sur le site que vous souhaitez visiter avant d'envoyer vos données.

ZP ARLON/ ATTERT /HABAY/ MARTLANGE
www.police.be/5297
063/60.85.00

ZP SUD-LUXEMBOURG
www.police.be/5298
063/21.04.60

ZP GAUME
www.police.be/5299
063/60.81.30

ZP FAMENNE ARDENNE
www.police.be/5300
084/31.03.11

ZP CENTRE ARDENNE
www.police.be/5301
061/24.12.11

ZP SEMOIS ET LESSE
www.police.be/5302
061/46.57.60

Ou appelez le 101

SERVICE PUBLIC FÉDÉRAL INTÉRIEUR SÉCURITÉ + PRÉVENTION
www.besafe.be/fr

SAFEONWEB
www.safeonweb.be/fr

SE PROTÉGER EN LIGNE C'EST CYBER SIMPLE !
www.cybersimple.be/fr

POINT DE CONTACT POUR FRAUDES, TROMPERIES, ARNAQUES ET ESCROQUERIES
www.pointdecontact.belgique.be/meldpunt/fr/bienvenue

Police

ESCROQUERIE

N'EN PAYEZ PAS LE PRIX!

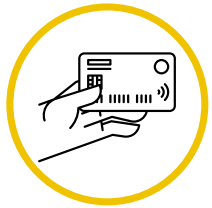
CYBERCRIMINALITÉ

A l'initiative du Gouverneur
et de la Police intégrée de la Province de Luxembourg

Police

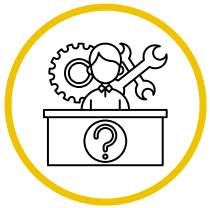
Si c'est trop beau pour être vrai, c'est que ça ne l'est pas

Bonjour, je suis Tom de la Commission européenne. Vous avez droit à une prime en raison de la crise actuelle. Puis-je avoir vos données bancaires?



NON → Fraude au digipass

Quelqu'un essaie de vous voler vos données bancaires pour effectuer un paiement au départ de votre compte. Très souvent, l'escroc se fait passer pour une firme ou une institution (ex: ministère, mutualité, etc.) par téléphone et vous propose de vous offrir de l'argent (prime covid, prime énergie, remboursement santé, etc.) avant de vous demander vos coordonnées bancaires et d'utiliser votre digipass.



Hello, votre ordinateur présente des problèmes de sécurisation et a été bloqué. Pour les résoudre à distance, contactez Microsoft au +1 -0970160158

NON → Fraude au service d'assistance / Helpdesk

La victime reçoit un message (souvent en anglais) pour l'effrayer qui lui indique qu'elle aurait un problème technique grave avec un service particulier (ex: Microsoft, Windows, banque, ...) et est invitée à effectuer certaines transactions via le « helpdesk » de ce service, par téléphone ou en téléchargeant une application.

Salut, c'est Marc, puis-je te parler? Je suis en vacances et mon portefeuille a été volé. Peux-tu m'envoyer de l'argent? Ou encore: Salut, j'aimerais tellement te rejoindre mais ma maman est très malade. Peux-tu m'envoyer de l'argent?

NON → Fraude à la demande d'aide/aux sentiments/à l'amitié

La victime est contactée par e-mail, par sms ou via les réseaux sociaux, vraisemblablement par un proche, un parent ou un ami, qui a besoin d'une aide financière urgente. Souvent, le contact s'est fait usurper son profil ou son adresse mail.

Bonjour, cet article est-il toujours disponible? Le prix me convient mais je suis une personne à mobilité réduite donc je vais demander au service DPD de venir retirer l'article et je vous fais un virement bancaire.

NON → Fraude à l'achat, à la vente et à la location ou faux web shop

Il s'agit d'escroqueries liées à des transactions commerciales entre particuliers lors de vente de produits via des sites tels que "2ememain", Marketplace et assimilés. Ces escroqueries reprennent différents modus (fausses annonces de vente, faux sites de vente, faux acheteurs, etc.).

Quelques conseils

Ne donnez jamais suite à une demande d'utilisation de votre **Digipass** et ne communiquez jamais d'**information** liée à celui-ci ainsi que vos **données bancaires**.

Si une institution, firme ou même un particulier vous réclame de l'argent par téléphone ou en ligne, **ne payez pas**. Renseignez-vous auprès de la firme ou l'institution en question.

Ne vous fiez pas au numéro de téléphone qui s'affiche sur votre récepteur. Ce numéro a pu être aisément acheté sur internet.

N'ouvrez pas un **email** dont vous ne connaissez pas le correspondant et ne cliquez jamais sur un **lien inconnu**.

Créer des **mots de passe sécurisés** avec une combinaison de chiffres, de minuscules, de majuscules, de caractères spéciaux.

Vous pensez être victime d'une arnaque par téléphone, **raccrochez immédiatement**.

Ne donnez jamais suite aux demandes d'utilisation de **sociétés de transfert de fond comme Western Union, Ria Money Transfert, Money Trans, Money Gram**,... lors d'un contact téléphonique avec une personne inconnue. Ces sociétés ne sont à utiliser que si vous connaissez personnellement le destinataire.

N'ouvrez pas de **fichier** joint au **mail** qui vous semble **étrange**.

Soyez vigilant avant d'installer une **application gratuite** (Webapps), renseignez-vous sur sa fiabilité et dans le doute, ne l'installez pas.

N'utilisez jamais **itsme** pour une opération que vous n'avez pas **personnellement** demandée.

Pensez également à **signaler les messages suspects** à: **suspect@safeonweb.be**

Safeonweb.be

et https://pointdecontact.belgique.be/meldpunt/fr

Avec le soutien de la Direction générale Sécurité et Prévention