Police Wokra

Wezembeek-Oppem & Kraainem

Chemin du Moulin 20 - 1970 Wezembeek-Oppem - Tel.: 02 766 18 18

Heures d'ouverture

Du lundi au vendredi: 7 - 19h
Weekend et jours fériés: fermé

Avant-propos

Vous avez reçu un e-mail du notaire vous annonçant qu'une tante perdue de vue vous laisse tout son héritage ?
Vous avez rencontré un ex-militaire américain sur Facebook qui vous a fait tourner la tête et qui veut venir vous rendre visite en Belgique, à condition que vous envoyiez de l'argent pour les billets d'avion ?

Vous avez reçu un message de votre petite-fille disant qu'elle a un nouveau numéro de téléphone et qu'elle a besoin d'argent car elle a des problèmes ?

Il n'est pas toujours facile de reconnaître les e-mails suspects ou les arnaques sur Internet. Les cybercriminels sont de plus en plus ingénieux et il est donc de plus en plus difficile de distinguer les faux messages des vrais.
Dans les pages qui suivent, nous allons tenter de vous expliquer les différentes formes de cybercriminalité et comment vous pouvez les reconnaître, nous vous donnerons des conseils et nous vous dirons également quoi faire si vous en êtes victime.

Achats en ligne frauduleux

Il s'agit d'une forme d'escroquerie où vous entrez en contact avec l'escroc via une fausse annonce sur un site officiel (2ememain, Autoscout, Immoweb, etc.) ou via un site web totalement frauduleux. L'escroc se fait passer pour un vendeur et propose un produit, généralement à un prix anormalement bas. Une fois l'argent transféré, l'escroc disparaît de la surface de la terre.

Signaux d'alarme :
- Le prix est trop beau pour être vrai.
- Utilisation de méthodes de paiement alternatives telles que Western Union ou Moneygram.
- Contact via WhatsApp
- Utilisation d'intermédiaires.
- Français bancal et fautes de langue.
- Adresse électronique ou numéro de portable étranger.
- Offres via les réseaux sociaux.
- Que des produits populaires tels que les iPhones, Airpods, PS5, téléviseurs Oled, ...

Conseils :
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.
- N'utilisez que des sites web connus.
- Rencontrez-vous en vrai.
- Utilisez votre carte Visa ou Mastercard.
- Le site web ci-dessous vous donne des conseils utiles pour vérifier l'authenticité d'un site web : www.cecbelgique.be/themes/achats-sur-internet/faites-le-webshop-check
- Renseignez-vous sur les témoignages des utilisateurs.

Vente en ligne frauduleuse

L'escroc répond à une de vos annonces et discute rarement du prix. Ensuite, 4 scénarios sont possibles :
1. L'acheteur paie avec un faux chèque d'une banque étrangère. Vous recevez l'argent mais, par la suite, le chèque s'avère être un faux et la banque vous réclame l'argent. Votre article a alors déjà été envoyé...
2. L'acheteur paie un montant plus élevé, toujours avec un faux chèque, et demande le remboursement de la différence. Cette fois, en plus de perdre votre article, vous perdez de l'argent supplémentaire.
3. L'acheteur vous demande d'avancer de l'argent pour couvrir les frais de transport, par exemple. Vous devez régler cette somme au moyen d'un système de paiement alternatif. Après cela, l'acheteur disparaît et vous perdez votre argent.
4. L'acheteur envoie une fausse capture d'écran du paiement. Vous envoyez l'article, mais vous ne recevez jamais votre argent.

Signaux d'alarme :
- Aucune discussion sur le prix.
- Utilisation de méthodes de paiement alternatives telles que Western Union ou Moneygram.
- Contact via WhatsApp
- Captures d'écran des paiements.
- Vous devez avancer de l'argent.
- Utilisation d'intermédiaires.
- Français bancal et fautes de langue.
- Adresse électronique ou numéro de portable étranger.

Conseils :
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.
- N'envoyez rien tant que vous n'avez pas reçu l'argent.

Fraude par e-mail

La fraude par e-mail est une forme d'escroquerie qui consiste à envoyer des e-mails à partir d'une adresse e-mail piratée ou similaire à une adresse originale, pour ensuite réclamer un paiement ou une livraison. Il peut également s'agir de factures envoyées par e-mail avec un numéro de compte modifié sur lequel le versement doit être fait.

Signaux d'alarme :
- Une facture a été ajoutée et vous pouvez clairement voir qu'elle a été modifiée (Tipp-Ex, ratures, numéros de compte différents, ...).
- Français bancal et fautes de langue.
- Langage menaçant
- L'adresse électronique ou le numéro de compte ne sont pas les mêmes que d'habitude.
- L'expéditeur n'envoie normalement jamais ses factures par e-mail.
- Vous n'attendez aucune facture de la part de l'expéditeur.
- L'e-mail ne vous est pas personnellement adressé.
- L'e-mail se trouve déjà dans votre dossier Spam.

Conseils :
- Contactez l'expéditeur (pas via les coordonnées figurant dans l'e-mail).
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.

Fraude relative aux maisons de vacances

L'escroc se fait passer pour le propriétaire d'une maison de vacances à louer. Des photos de maisons de vacances existantes sont utilisées pour donner un aspect authentique. De faux sites internet peuvent également être utilisés. Une fois que vous avez payé, le propriétaire disparaît ou, pire encore, vous vous retrouvez devant la porte d'un complexe de bureaux en Espagne à la place de cette belle maison de vacances.

Signaux d'alarme :
- Le prix est trop beau pour être vrai.
- Français bancal et fautes de langue.
- Site web peu soigné.
- Réductions en cas de prise de décision rapide.
- Utilisation de méthodes de paiement alternatives telles que Western Union ou Moneygram.
- Le compte du propriétaire provient d'un pays différent de celui où se trouve la maison.

Conseils :
- Ne communiquez pas d'informations personnelles.
- Réservez par l'intermédiaire d'un organisme agréé.
- Faites des recherches via Google et lisez les avis.
- Recherchez l'adresse sur Google Maps.
- Vous pouvez également effectuer une recherche par images sur Google. Sur la page d'accueil de Google, cliquez sur « images » en haut à droite. Vous pouvez ensuite télécharger l'image de la maison ou copier l'URL. Si vous cliquez ensuite sur le bouton « Rechercher », vous obtiendrez une liste de toutes les pages où cette image apparaît.
- Interrompez tout contact et n'effectuez aucun paiement.

Whaling

Le whaling consiste pour l'escroc à se faire passer pour une de vos connaissances, par exemple pour votre fils ou votre petite-fille, et à vous contacter sur un numéro inconnu sous prétexte que son téléphone portable est cassé ou qu'il ou elle l'a perdu, ou encore que son numéro est bloqué, ...
La personne déclare être dans le besoin et demande qu'un paiement urgent soit effectué. L'argent sera remboursé dès que possible par la suite.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Une connaissance vous contacte par SMS ou WhatsApp pour effectuer un versement ? Bizarre, c'est le moins que l'on puisse dire !

Conseils :
- Contactez la personne sur son numéro d'appel habituel.
- Essayez d'entrer en contact avec la personne par d'autres moyens. Par le téléphone fixe, par l'intermédiaire de son ou de sa partenaire, ...
- N'effectuez jamais le paiement demandé. Il n'y a jamais de paiement qui ne peut attendre.
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.
- Il peut également arriver que le numéro d'appel habituel ait été piraté.

Fraude à l'investissement

En cas de fraude à l'investissement, les escrocs peuvent opérer de deux manières différentes.

1. La première méthode consiste à approcher les victimes spontanément, par démarchage téléphonique ou par courrier électronique, en leur proposant d'investir dans un produit particulier. Bien sûr, cela va de pair avec la promesse de faire des profits étonnamment élevés.
2. La deuxième méthode, qui est de plus en plus courante, consiste à utiliser des publicités frauduleuses via les réseaux sociaux et/ou via des sites web totalement fictifs.

Une fois que vous avez investi votre argent, vous n'avez plus de nouvelles des investisseurs ou ils vous promettent de vous reverser l'argent si vous effectuez un autre versement.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Vous êtes contacté de manière spontanée.
- Les bénéfices annoncés sont trop beaux pour être vrais.
- Sites web ou intermédiaires étrangers.
- Référence à des personnes connues.
- Demande de transfert d'argent vers l'étranger.
- Des paiements supplémentaires sont demandés.
- Vous devez « vous décider rapidement ».

Conseils :
- Ne communiquez pas d'informations personnelles.
- Vérifiez l'identité de la personne ou de l'entreprise.
- N'effectuez aucun versement vers l'étranger, en particulier en dehors de l'UE.
- Vous pouvez vérifier s'il s'agit d'une escroquerie en effectuant un test sur le site www.fsma.be/fr/attention-aux-fraudes.

Phishing

Le phishing consiste à essayer de trouver vos coordonnées bancaires en vous attirant sur un faux site internet, qui est généralement une copie d'un vrai site. Vous devez ensuite vous connecter avec votre nom d'utilisateur et votre mot de passe ou avec votre lecteur de carte et votre carte bancaire. L'escroc peut ainsi s'emparer de vos coordonnées avec toutes les conséquences que cela implique.
En général, les victimes sont trompées grâce à un faux e-mail ou un faux message au nom d'institutions de confiance telles que des banques, des organismes gouvernementaux, la police, ... Le message contient généralement un lien vers un site internet sur lequel vous devez vous connecter.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Il est fait référence à un site qui ressemble à celui d'origine.
- L'e-mail ne vous est pas personnellement adressé.
- L'e-mail se trouve déjà dans votre dossier Spam.
- Le ton employé est marqué par l'urgence.
- Message via WhatsApp.
- Vous devez télécharger un outil.

Conseils :
- Les organismes officiels tels que les banques, les services gouvernementaux, la police, itsme, etc. ne vous demanderont jamais de vous connecter par e-mail ou par SMS, et encore moins en utilisant votre lecteur de carte et votre carte bancaire.
- Ne donnez jamais votre code PIN et n'effectuez aucune transaction en utilisant un lecteur de carte.
- De manière générale, ne partagez jamais vos codes ou vos mots de passe personnels.
- Au lieu de cliquer sur un lien, recherchez vous-même le bon site web.
- Si vous avez cliqué sur le lien et que vous avez un doute, vérifiez le nom de domaine dans l'url du site web. Vous le trouverez en haut de la page. Le nom de domaine, le mot avant .be, .com, .org, .eu, ... et avant la toute première barre oblique « / », est-il vraiment le nom de l'organisation ?
- Le nom de domaine officiel se trouve-t-il après le @ dans l'adresse électronique ?
- Contactez l'organisme via le numéro de téléphone officiel.
- Ne communiquez pas d'informations personnelles.
- Ne répondez pas à l'e-mail ou au message.
- N'ouvrez pas les pièces jointes.
- N'envoyez aucune photo de votre carte bancaire ou de votre carte d'identité.
- En cas de doute, demandez de l'aide.

Fraude à l'amitié

Les escrocs tentent de plus en plus de jouer sur les sentiments de leurs victimes pour leur soutirer de l'argent. Les prises de contact peuvent commencer de différentes manières : par un spam, sur un site de rencontre, sur les réseaux sociaux, dans un espace de chat, ...
Pendant plusieurs semaines, ils essaient de nouer une relation de confiance et, lorsque celle-ci est suffisamment solide, ils vous demandent de l'argent. Cet argent est ensuite censé servir à un voyage vers la Belgique, à acheter des vêtements, à prendre soin de la famille, à payer des frais d'hospitalisation, à obtenir un héritage. Et ainsi de suite.
Après avoir versé plusieurs sommes d'argent, la personne devient soudainement silencieuse et vous réalisez qu'elle n'a en réalité jamais existé.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Des demandes d'ami sur les réseaux sociaux qui sont trop belles pour être vraies.
- Utilisation de méthodes de paiement alternatives telles que Western Union ou Moneygram.

Conseils :
- N'acceptez aucune demande de la part d'inconnus sur les réseaux sociaux.
- Cherchez le nom de cet « ami » sur Google.
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.
- Dénoncez l'escroc.

Fraude « Wangiri »

Vous recevez un SMS d'un numéro étranger, généralement en français. Vous avez apparemment gagné quelque chose et vous devez appeler un certain numéro pour recevoir votre prix. Une autre méthode consiste à recevoir un appel d'un numéro étranger et, avant même que vous puissiez décrocher, l'appel s'arrête. Ils espèrent évidemment que vous rappellerez.
Dans les deux cas, il s'agit d'un numéro payant très cher où l'on essaie de vous garder en ligne le plus longtemps possible.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Utilisation de numéros d'appel étrangers.
- Voix d'ordinateur et musique d'attente.

Conseils :
- Ne répondez pas aux SMS.
- Ne rappelez pas.
- Bloquez le numéro sur votre smartphone.

Ransomware

Un ransomware est un type de logiciel malveillant qui verrouille vos fichiers, voire l'ensemble de votre système, par le biais du cryptage. Les criminels vous donnent ensuite le choix de faire affaire avec eux ou de renoncer à vos fichiers.
Les ransomwares s'introduisent généralement par un e-mail contenant une pièce jointe infectée. Cependant, ils peuvent également s'introduire via de sites pornographiques ou de sites de téléchargement illégaux. Lorsque vous cliquez sur cette pièce jointe, un certain cheval de Troie commence à crypter vos fichiers. Vous recevez ensuite un message sur votre écran indiquant que vos fichiers ont été cryptés. Il vous est par la suite demandé de transférer une somme d'argent ou des bitcoins dans un délai de x heures pour que les fichiers soient décryptés. Si vous ne le faites pas, tous vos fichiers seront perdus à jamais.

Signaux d'alarme :
- Un message sur votre écran vous indique que votre système a été crypté.
- Des e-mails suspects accompagnés de pièces jointes.

Conseils :
- Faites des sauvegardes de vos fichiers.
- N'ouvrez pas les e-mails ou les pièces jointes provenant d'expéditeurs suspects.
- Assurez-vous d'avoir un bon logiciel antivirus.
- Mettez régulièrement vos systèmes et logiciels à jour.
- www.nomoreransom.org

Si vous en êtes toutefois victime :
- Signalez dès que possible les faits à la police.
- Ne payez rien.
- Prenez une photo de l'écran.
- Prenez une photo de l'adresse ou du numéro de compte du cryptowallet/Bitcoin.
- Donnez toute information sur le système infecté.
- Donnez des informations sur la manière dont le virus a pu s'introduire.
- Éteignez complètement l'ordinateur et déconnectez-le d'Internet et des disques durs externes.
- Il est parfois possible de décrypter les fichiers. Certaines de ces clés de décryptage se trouvent sur le site www.nomoreransom.org.

Piratage

Le piratage consiste à s'introduire dans un système ou dans un réseau informatique. Les pirates utilisent des virus, des logiciels espions ou ont également recours au piratage du code d'un système. L'objectif est généralement de prendre le contrôle du système, de voler des données ou de rendre le système et les données inutilisables.
Le piratage des comptes en ligne concerne les comptes en ligne tels que les messageries électroniques, les réseaux sociaux, les comptes sur des sites de vente, ... Cela arrive généralement parce que votre mot de passe est trop simple ou parce que le pirate connaît la réponse à votre question de sécurité. Une fois votre compte piraté, ils peuvent utiliser vos informations personnelles, envoyer des spams en votre nom, escroquer des personnes en votre nom, effectuer des achats ou commettre d'autres actes criminels.

Signaux d'alarme :
- Votre système ou votre réseau fonctionne de manière étrange.
- Votre système est bloqué.
- De faux e-mails circulent en votre nom.
- Vous ne parvenez plus à accéder à vos comptes.

Conseils :
- Assurez-vous d'avoir un mot de passe suffisamment fort : au moins 8 caractères, majuscules et minuscules, symboles, ...
- N'utilisez pas de mots de passe évidents tels que le nom de vos enfants, de vos animaux domestiques, votre date de naissance, ...
- Utilisez la vérification en deux étapes pour vos mots de passe
- Installez un bon logiciel antivirus et mettez vos systèmes régulièrement à jour.

Sextorsion

L'escroc vous aborde sur les réseaux sociaux ou vous l'avez rencontré dans un espace de chat. Vous commencez à parler, et une chose en entraînant une autre, la conversation devient vite érotique. Vous échangez des messages érotiques et il vous convainc de partager des photos ou des vidéos compromettantes de vous-même. Ensuite, les extorqueurs menacent de diffuser les images si vous ne leur versez pas de l'argent.
Il est également possible que vous receviez un e-mail indiquant que l'escroc possède des images nues de vous et qu'il les publiera si vous ne transférez pas une certaine somme d'argent. Ce n'est pourtant pas le cas, mais par peur, vous payez quand même.

Signaux d'alarme :
- Français bancal et fautes de langue.
- Des demandes d'ami sur les réseaux sociaux qui sont trop belles pour être vraies.

Conseils :
- N'acceptez aucune demande de la part d'inconnus sur les réseaux sociaux.
- N'échangez pas de contenu érotique en ligne.
- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.
- Dénoncez l'escroc.

Fraude nigériane

En tant que victime potentielle, vous êtes contacté par une personne de l'étranger qui se fait passer pour :

- Un héritier d'une personne connue ou d'un riche homme d'affaires ;
- Quelqu'un qui est gravement malade et qui n'a pas d'héritier ;
- Un employé de banque qui a découvert une somme d'argent qui vous revient.

Il s'agit donc à chaque fois de quelqu'un qui possède une grosse somme d'argent et qui, en quelque sorte, chercher à la faire sortir du pays. En échange de votre aide, vous recevez un pourcentage de cette somme. Cette aide consiste à avancer une somme d'argent pour des frais de notaire, des droits de douane, des taxes, etc. Chaque fois que vous payez, d'autres frais apparaissent et, bien sûr, vous ne recevez jamais rien en retour. Après avoir effectué quelques versements, vous n'avez plus de nouvelles de l'autre partie.

Signaux d'alarme :

- Un inconnu vivant à l'étranger vous propose de l'argent ?
- Il s'agit généralement de millions d'euros ou de dollars.
- Il s'agit généralement d'une personne issue d'un pays d'Afrique ou d'Asie.
- Utilisation de méthodes de paiement alternatives telles que Western Union ou Moneygram.
- L'e-mail ne vous est pas personnellement adressé.
- Français bancal et fautes de langue.

Conseils :

- Ne communiquez pas d'informations personnelles.
- Interrompez tout contact et n'effectuez aucun paiement.

Et si vous vous faites quand même avoir ?

Malgré toutes les précautions que vous prenez, toutes les mises en garde que vous suivez et toutes les informations sur les escroqueries dont vous disposez, les choses peuvent toujours mal tourner et vous pouvez devenir victime d'une escroquerie. Vous ne serez pas le premier et certainement pas le dernier.
Les gens ont souvent honte d'avouer qu'ils ont été victimes d'une escroquerie. Il est cependant important de prendre les mesures nécessaires non seulement pour pouvoir être aidé, mais aussi pour que d'autres personnes ne deviennent pas inutilement victimes à leur tour.
Il est important de faire une distinction entre le fait d'avoir perdu de l'argent ou non :

Vous n'avez pas perdu d'argent ?

- Il n'est alors pas nécessaire de faire un signalement à la police.
- Transférez le message frauduleux que vous avez reçu à verdacht@safeonweb.be. Cela permet de bloquer les faux sites web ou les fausses adresses électroniques.
- Changez vos mots de passe si nécessaire.

Vous avez perdu de l'argent ou vous avez été piraté ?

- Appelez immédiatement Card Stop (078 170 170) si vous avez communiqué vos coordonnées de paiement.
- Contactez votre banque. Il est éventuellement possible de suspendre un paiement.
- Faites un signalement à la police.

Qu'apporter en cas de déclaration?

- Ordinateur portable et/ou smartphone.
- L'URL exacte du site web frauduleux, si possible une capture d'écran.
- Captures d'écran des messages, e-mails, réseaux sociaux, ...
- Données d'identité, adresse électronique, numéro de compte, numéro d'appel, ... du suspect.
- Résumé des transactions frauduleuses.
- Informations sur les biens achetés à votre nom.
- Toute autre information relative à l'escroquerie, il est préférable d'en avoir trop que trop peu.

Liens utiles

- www.safeonweb.be - Téléchargez aussi l'application pour bénéficier de notifications sur de nouveaux risques.
- Envoyez vos mails suspects à : suspect@safeonweb.be.
- Escroqueries, fraude ou arnaques: pointdecontact.belgique.be
- www.nomoreransom.org
- www.cert.be
- www.cecbelgique.be
- www.clicksafe.be
- www.cybersimple.be
- www.ccb.belgium.be
- www.safeinternetbanking.be
- www.besafe.be