Vous avez acheté en ligne un produit ou un service sans recevoir en retour, malgré vos rappels, le bien pour lequel vous avez payé ? Ne cherchez pas, vous avez hélas été victime d'une escroquerie.

La définition de l'escroquerie et ses conséquences sont reprises à l'article 496 du Code pénal.

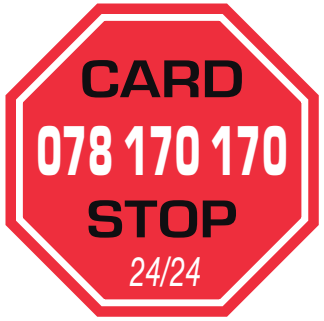
Que faire si vous avez été victime ?

Déposez plainte auprès d'un commissariat en communiquant idéalement les informations suivantes :

- ☑ Référence du (des) transfert(s) d'argent effectué(s) ;
- ☑ Adresse de messagerie, numéro de téléphone et pseudo utilisés par le(s) escroc(s) ;
- ☑ Copie des courriels et/ou SMS échangés ;
- ☑ Tout autre renseignement permettant d'identifier le ou les escrocs.

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



Numéros de téléphone utiles

Commissariats ouverts 24h/24, 7j/7

Direction de Proximité et d'Intervention CENTRE
1000 Bruxelles, rue du Marché au Charbon 30
02/279.77.11

LAEKEN
1020 Bruxelles, boulevard Emile Bockstael 246
02/279.88.10

IXELLES - LOUISE
1050 Ixelles, rue du Collège 1
02/279.84.16

NEDER-OVER-HEEMBEEK/HAREN
1120 Bruxelles, avenue de Versailles 130
02/279.81.10 & **02/279.89.10**

Liens utiles

Police Bruxelles CAPITALE Ixelles
www.polbru.be

Service Public Fédéral Intérieur Sécurité & Prévention
www.besafe.be/fr

Safeonweb.be
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
https://meldpunt.belgie.be

CYBER-CRIMINALITÉ

Prévention

Police

Bruxelles CAPITALE Ixelles

Quelques conseils pour vous protéger

Antivirus

Équipez votre ordinateur d'un logiciel antivirus.

Mise à jour

Effectuez régulièrement les mises à jour de votre système d'exploitation et de votre antivirus.

Sauvegarde

Faites régulièrement des sauvegardes de vos données sur un support externe.

Programmes

Installez uniquement des programmes ou applications diffusés par un site officiel.

Pièces jointes suspectes: ne pas ouvrir !

Liens suspects : ne cliquez pas dessus !

Vie privée

Ne communiquez jamais vos informations personnelles (identité, coordonnées bancaires, codes, etc.) à des inconnus.

Mots de passe forts

Veillez à choisir des mots de passe compliqués avec symboles, chiffres, majuscules et minuscules. Pour davantage de facilité de mémorisation, utilisez un gestionnaire de mots de passe.

Opérations bancaires

Utilisez le navigateur sécurisé disponible avec votre antivirus. Pensez à contrôler de manière régulière vos extraits de compte et relevés de carte de crédit afin de déceler toute transaction frauduleuse.

Réseaux sociaux

Configurez les paramètres de confidentialité afin de protéger vos contenus. Aussi, méfiez-vous des « demandes d'amitié » provenant de personnes inconnues.

Quelques exemples d'escroquerie

Phishing

Tentative d'accéder à vos données confidentielles en se faisant passer pour une banque ou une administration.

Sextorsion ou extorsion à l'aide d'images à caractère sexuel

Des escrocs parviennent à vous convaincre d'envoyer des photos intimes qu'ils menacent ensuite de diffuser si vous ne leur versez pas de l'argent. Ne partagez pas de photos intimes sur Internet et les réseaux sociaux et encore moins avec des personnes inconnues.

Arnaque par sextorsion

Des escrocs affirment avoir piraté votre ordinateur et avoir pris des photos compromettantes de vous en train de regarder un film pornographique. Ils vous menacent de les diffuser à moins que vous ne vous acquittiez d'une certaine somme d'argent.

Ransomware

Programme malveillant utilisé pour obtenir une rançon de la part de la victime en retenant ses données personnelles.

Le cyberharcèlement

Harcèlement commis sur Internet ou sur les réseaux sociaux pouvant prendre différentes formes telles que la création de faux profils, la diffusion de fausses rumeurs, de messages d'insulte ou malveillants.

Spamming

Message publicitaire pouvant comporter un risque tel que le vol de vos données confidentielles (cf. phishing), l'infection de votre ordinateur par un logiciel espion contenu dans le message, etc.

Hacking

Accès non autorisé à votre système informatique à des fins frauduleuses.

Fraude informatique

Consiste à obtenir de votre part des biens ou des fonds au moyen de belles promesses, paroles ou propositions. Généralement, il s'agit d'une somme d'argent que la victime paie pour un bien inexistant (transactions financières, loteries ou jeux de hasard, achats et ventes sur Internet, etc.).

Certains sites tels que 2ememain.be, Marketplace de Facebook, etc. sont devenus des lieux de prédilection pour les escrocs.

Vous pouvez retrouver d'autres informations relatives aux escroqueries sur le site de la Police Fédérale :

www.police.be/5998/fr/actualites/fraude-internet

Editeur responsable : Chef de corps Michel Goovaerts