

FRAUDE À L'ÉMOTION (ROMANCE SCAM)

Les fraudes à l'émotion (ou arnaques aux sentiments/amitié) sont des escroqueries manipulant les sentiments (amour, pitié, urgence) pour soutirer de l'argent. Les fraudeurs créent de faux profils sur les réseaux sociaux ou sites de rencontre, établissant un lien de confiance durable avant de demander des fonds pour de prétendues urgences médicales, voyages ou frais juridiques.

Exemple concret : Pierre Garnier

Une septuagénaire belge est victime depuis début 2024 d'un escroc qui utilise des photos et de fausses vidéos du chanteur pour créer un lien sentimental.

La victime a déjà viré plus de 7 000 euros à l'escroc, malgré les avertissements de ses enfants. La dame est convaincue d'échanger avec le vrai chanteur et continue d'envoyer de l'argent dès qu'elle reçoit sa pension, se retrouvant dans une situation financière et personnelle difficile.

La famille de la septuagénaire a déposé plainte pour escroquerie en ligne et a lancé un appel à l'aide, espérant une intervention du vrai Pierre Garnier.

Conseils pratiques



Soyez vigilants à ce que vous affichez comme information ou publiez sur les réseaux sociaux et les sites de rencontres.

Les escrocs pourraient en effet utiliser ces informations pour mener à bien leur escroquerie.



N'envoyez jamais d'argent à une personne avec laquelle vous n'avez communiqué qu'en ligne ou par téléphone.



N'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter.



Prenez le temps de connaître votre interlocuteur en lui posant de nombreuses questions et en évaluant la cohérence de ses réponses.



Méfiez-vous si la personne tente de vous isoler de vos proches.

SI VOUS AVEZ ÉTÉ VICTIME :

Si malgré tous ces conseils, les auteurs ont pu accéder à votre compte bancaire, contactez les instances suivantes, dans cet ordre :

1) Card Stop (078 170 170):

Gratuitement accessible 24/7.

• Bloquez la carte de banque ou vos applications de paiement (Payconiq, Apple Pay, Google Pay)

2) Banque

- Bloquez vos comptes.
- Obtenez des preuves, en particulier des relevés de compte.
- Faites bloquer l'accès à l'application bancaire.
- Appelez le service fraude de la banque (accessible 24 heures sur 24, 7 jours sur 7).

3) Police locale

- Déposez une plainte, avec des preuves.
- Prenez autant de captures d'écran que possible.

Si d'autres données personnelles (par exemple, les données de la carte d'identité, du passeport, du permis de conduire) sont tombées entre les mains des escrocs, il est essentiel que vous le signaliez à la police le plus rapidement possible.

Dans le cas de documents d'identité, adressez-vous à Doc Stop (00800 2123 2123 ou +32 2 518 2123 depuis l'étranger).



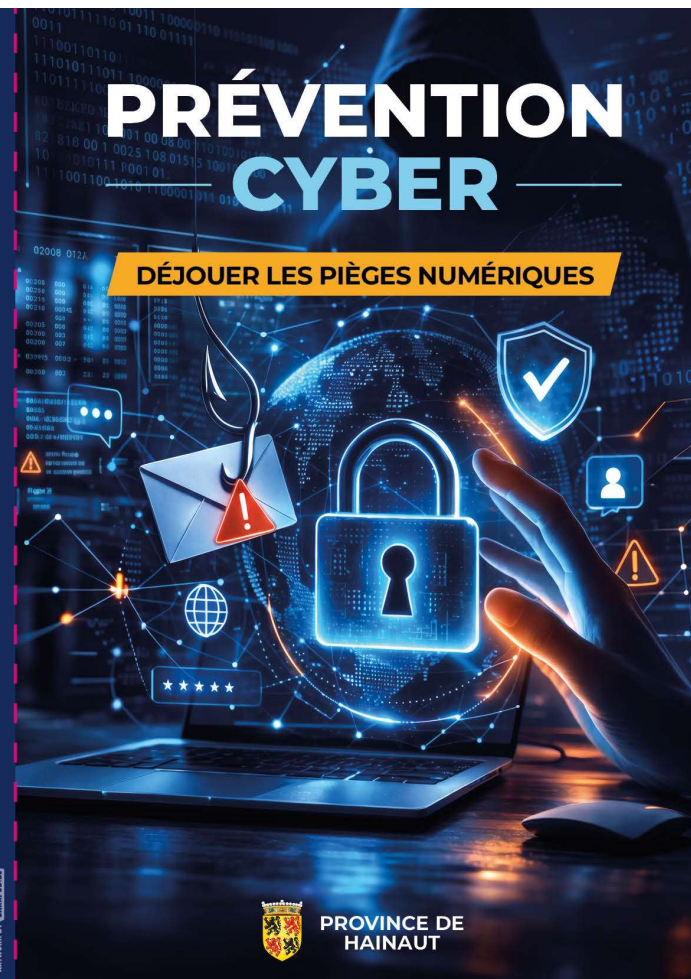
**Bureau provincial
Prévention du vol**

☎ 071 244 707

✉ bppv.hainaut@gmail.com

PRÉVENTION CYBER

DÉJOUER LES PIÈGES NUMÉRIQUES



**PROVINCE DE
HAINAUT**

PRÉVENTION CYBER

Cette brochure présente un aperçu non exhaustif de plusieurs types d'escroqueries en ligne courantes.

Vous y retrouverez également : des conseils pour reconnaître les fraudes, des mesures de prévention, les démarches à effectuer si vous êtes victime.

COMMENT RECONNAÎTRE UNE TENTATIVE DE FRAUDE

Les tentatives de fraude en ligne sont de plus en plus difficiles à repérer. Les conseils suivants peuvent vous aider à démasquer les messages suspects :

Est-ce inattendu ?

Vous recevez un message de cet expéditeur sans raison : vous n'avez rien acheté, vous n'avez pas eu de contact depuis longtemps, etc. Assurez-vous de vérifier davantage.

Est-ce urgent ?

Gardez votre calme : Vous connaissez cet «ami dans le besoin» ? Avez-vous vraiment reçu un premier rappel de paiement ?

Connaissez-vous l'expéditeur ?

Vérifiez l'adresse e-mail, y compris les fautes d'orthographe. Mais attention : une adresse e-mail légitime n'est pas une garantie.

Trouvez-vous la question étrange ?

Un organisme officiel ne vous demandera jamais votre mot de passe, vos coordonnées bancaires ou des informations personnelles par e-mail, SMS ou téléphone.

Où mène le lien sur lequel vous devez cliquer ?

Contrôlez le nom de domaine de l'URL du site. Le nom de domaine, c'est le mot qui précède .be, .com, .eu, .org et la première barre oblique « / ». Est-ce que ce dernier correspond réellement au nom de l'organisation ?

Dans le lien www.safeonweb.be/conseils, le domaine est «safeonweb». Dans le lien www.safeonweb.conseils.be/safeonweb, le domaine est «conseils». Ce lien vous dirige vers un site Internet différent.

Le message se trouve-t-il dans votre dossier Spam/Junk ?

Si oui, redoublez de prudence. Vous pouvez également marquer vous-même les messages suspects comme spam ou indésirable et avertir les autres.

Source : safeonweb

LE PHISHING

Le phishing (ou hameçonnage) est une technique de fraude en ligne extrêmement répandue utilisant des messages frauduleux (e-mails, SMS, réseaux sociaux) qui imitent des personnes ou institutions de confiance (banques, administrations, services). L'objectif est de manipuler la victime pour qu'elle révèle des données personnelles, bancaires ou des mots de passe.

Conseils pratiques :

- Méfiez-vous des offres trop belles pour être vraies.
- Vérifiez l'adresse mail de l'expéditeur.
- Apprenez à reconnaître les liens frauduleux : surfersanscauci.safeonweb.be
- Vérifiez l'information sur le site officiel de l'institution.
- Transmettez les messages suspects à suspect@safeonweb.be



LES FRAUDES AUX INVESTISSEMENTS :

La fraude à l'investissement est une forme d'escroquerie où des criminels tentent de vous convaincre d'investir de l'argent dans des produits financiers inexistantes ou faux (crypto, forex,...). Ils promettent souvent des rendements élevés avec peu de risques, mais en réalité il s'agit d'un piège pour voler votre argent. Souvent, ces fraudeurs disparaissent sans laisser de trace après avoir reçu votre argent.

Méthodes les plus courantes utilisées par les fraudeurs :

Médias sociaux et publicités : Ils font de la publicité sur Facebook, Instagram ou YouTube avec des vidéos professionnelles ou des visages célèbres ou ils vous approchent via un message personnel sur l'un de vos médias sociaux.

Faux sites web ou fausses plateformes : Ils créent de faux sites web professionnels qui semblent légitimes, y compris de fausses critiques.

Mails : Vous recevrez un mail contenant une invitation exclusive à participer à un investissement prometteur.

Sites et applications de rencontre : Ils établissent d'abord un lien de confiance par le biais d'une plateforme de rencontre, puis amènent subtilement la conversation sur l'investissement (pig butchering-fraude).

WhatsApp ou SMS : Parfois, ils se font passer pour un ami, un membre de la famille ou un «coach en investissement» par le biais de messages.

Téléphone : Vous recevez un appel non sollicité vous proposant une offre d'investissement soi-disant intéressante.

Conseils pratiques :

- Soyez critique :**
- Prenez toujours le temps de dissiper vos doutes.
 - N'effectuez pas de paiements précipités.
 - Protégez vos données personnelles.

LE VISHING

Les arnaques par téléphone, aussi appelées vishing, sont en nette augmentation. Les fraudeurs utilisent différents scénarios pour inciter les citoyens à agir dans l'urgence et à divulguer des informations sensibles ou à effectuer des paiements.

Exemples concrets de Vishing

Appels provenant de numéros étrangers

De nombreux citoyens reçoivent des appels de numéros inconnus, souvent avec un indicatif étranger. Il s'agit généralement de messages automatisés ou de faux collaborateurs d'organismes connus qui évoquent un problème urgent : activité suspecte, compte bloqué... Le but est de pousser la victime à rappeler le numéro ou à communiquer des informations personnelles.

La fraude Wangiri : un appel très bref

Dans certains cas, l'escroc se contente de faire sonner le téléphone une seule fois. Par curiosité ou par inquiétude, la victime rappelle le numéro. Il s'agit alors souvent d'un numéro surtaxé, parfois situé à l'étranger. Chaque appel peut engendrer des frais importants.

Faux appels de Card Stop

Un message automatisé indique qu'une transaction suspecte a été détectée et invite la victime à confirmer ses données bancaires ou son code. Rappel important : Card Stop ne vous demandera jamais vos codes ou informations personnelles par téléphone.

Que faire si vous recevez un appel téléphonique inattendu ?



Ne donnez jamais de détails personnels, de mots de passe, de codes de carte bancaire ou de codes de réponse du digipass via téléphone.

Ne rappelez jamais des numéros inconnus. Ne répondez jamais à des numéros que vous ne connaissez pas.

Ne croyez pas tout ce qu'on vous raconte au téléphone. Votre banque, la police ou le gouvernement ne vous demandera jamais vos codes par téléphone.