# Boîte à outils : inspiration prévention cyber

ibz Intérieur Binnenlandse Zaken

.be

Cette première version de la boîte à inspiration prévention cyber vous donne un aperçu non exhaustif des principaux types d'escroqueries en ligne, des conseils aux victimes, quelques astuces de prévention, les organisations supralocales auxquelles vous pouvez vous adresser et quelques pratiques locales inspirantes. Cette boîte à outils s'adresse en priorité aux autorités locales, peu familiarisées avec la cyberprévention mais de plus en plus confrontées à celle-ci. Le niveau local peut faire la différence en permettant une approche globale contre la cybercriminalité.

Nous vous souhaitons beaucoup de plaisir de lecture.

## Principaux types d'escroqueries en ligne

### Phishing

Les escroqueries en ligne par le biais de faux courriels, sites web ou messages. Les cybercriminels tentent de tirer parti d'une chose à laquelle la victime croit ou d'une personne qu'elle connaît et en qui elle a confiance. Ils essaient aussi souvent de jouer sur la peur. Plus d'informations : https://campagne.safeonweb.be/fr/phishing

### Fraude au service d'assistance

Forme d'escroquerie où les fraudeurs se font passer pour des employés du service d'assistance de grandes entreprises bien connues (banques et entreprises technologiques, par exemple). Ils disent qu'il y a un problème majeur et qu'il est urgent d'agir. Plus d'informations : Je suis contacté par un inconnu pour un problème de pc | Safeonweb

### Fraude à l'émotion : Fraude à la demande d'aide

Les fraudeurs se font passer pour une connaissance ou un être cher de leur victime. Ils demandent une aide financière par le biais de messages électroniques, de SMS ou d'applications. Pour gagner la confiance, ils utilisent des informations personnelles sur les personnes connues/chères ou capables de trouver ou d'acheter (également connu sous le nom d'ingénierie sociale). Plus d'informations : Méfiez-vous de la fraude à la demande d'aide financière urgente d'un soi-disant proche | Febelfin

### Fraude à l'émotion : Fraude à la demande d'aide

Les escrocs prennent contact avec leurs victimes potentielles qu'ils soupçonnent d'être seules ou d'avoir un besoin urgent d'amour. Contrairement à la plupart des autres formes d'escroquerie en ligne, l'auteur investit beaucoup de temps pour gagner la confiance de la victime, après quoi il lui demande de l'argent au fil du temps. Ainsi, une soi-disant situation d'urgence sera souvent utilisée comme excuse dans ce type d'escroquerie. Plus d'informations : Les fraudes à l'amitié | Trop Beau Pour Être Vrai (tropbeaupouretrevrai.be)

### Fraude aux comptes à sécurité renforcée

Ici, les escrocs abordent généralement les citoyens en deux étapes : ils envoient d'abord un message de phishing pour extraire les codes bancaires personnels. C'est ainsi qu'ils essaient d'accéder au compte bancaire. Les escrocs appellent ensuite la personne. Ils se font ensuite passer pour un employé de banque et demandent de transférer de l'argent sur un compte soi-disant nouveau et sécurisé. Plus d'informations : Fraude aux comptes à sécurité renforcée : nos conseils ! | Febelfin

**Fraude à l'achat et à la vente**

La fraude à l'achat consiste à transférer de l'argent à une personne ou à une entreprise sans recevoir le service ou le produit pour lequel il a été payé. Dans la fraude à la vente, les marchandises sont livrées mais le destinataire ne les paie pas. À cet égard, les sites web d'occasion sont un endroit populaire pour commettre ces délits.

Plus d'informations : Gare aux escrocs sur les sites de ventes en ligne | Safeonweb

**Fraude au CEO**

La fraude au CEO est une forme d'escroquerie dans laquelle les cybercriminels contactent une entreprise (par téléphone ou par courrier électronique) pour lui demander d'effectuer un paiement important

vers leur compte en banque. Les cybercriminels prennent l'identité du CEO, du directeur financier ou d'une personne de confiance et demandent à un employé des finances ou de la comptabilité d'effectuer un paiement urgent.

Plus d'informations : La fraude au CEO - Mieux vaut prévenir que payer | Centre pour la Cybersécurité Belgique (belgium.be)

## Assister les victimes

Si les auteurs ont pu accéder au compte bancaire de la victime, celle-ci doit contacter les instances suivantes, dans cet ordre :

1) Card Stop (078 170 170):
   - Gratuitement accessible 24/7
   - Bloquer la carte de banque

2) Banque
   - Bloquer les autres moyens de paiement
   - Obtenir des preuves, en particulier des relevés de compte
   - Faire bloquer l'accès à l'application bancaire : https://cardstop.be/fr/home/Je-veux-bloquer/Bloquez-via-lemetteur.html
3) Police locale
   - Pour déposer une plainte, avec des preuves.
   - Conseiller aux victimes de prendre 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 les victimes le signalent à la police le plus rapidement possible. Dans le cas de documents d'identité, la victime doit s'adresser à Doc Stop (00800 2123 2123 ou +32 2 518 2123). Plus d'informations : DOCSTOP - CHECKDOC

DOC STOP 24/24 00800 2123 2123 +32 2 518 2123

CARD 078 170 170 STOP 24/24

# Principaux conseils de prévention

## Remarques générales

Les tentatives de fraude en ligne sont de plus en plus difficiles à repérer. Dans la plupart des formes d'escroquerie en ligne, les auteurs utilisent un modus operandi similaire, mais il est souvent présenté de manière différente. Les conseils suivants de SafeOnWeb peuvent vous aider à démasquer les messages suspects :

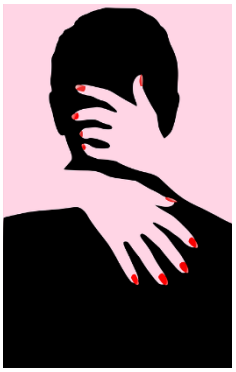
- **Est-ce inattendu ?**
  Vous recevez un message de cet expéditeur sans raison : vous n'avez rien acheté, vous n'avez pas eu de contact depuis longtemps, etc. Assurez-vous de vérifier davantage.
- **Est-ce urgent?**
  Gardez votre calme : Vous connaissez cet "ami dans le besoin" ? avez-vous vraiment reçu un premier rappel de paiement ? Vous connaissez cet "ami dans le besoin" ?
- **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 ?**
  Passez votre souris sur le lien. Le nom de domaine, le mot pour .be, .com, .eu, .org, … et pour le tout premier slash « / », est-il vraiment le nom de l'organisation ?
- **Êtes-vous adressé personnellement?**
  Les messages avec des titres généraux et vagues, ou votre adresse e-mail en guise de salutation, doivent vous inspirer la méfiance méfiants.
- **Le message contient-il de nombreuses erreurs de langue ?**
  Même si les cybercriminels chevronnés s'expriment dans un langage correct, des erreurs de langage ou une langue étrangère peuvent indiquer un message suspect.
- **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.
- **Est-ce que quelqu'un essaie de vous rendre curieux?**
  N'importe qui serait curieux de recevoir des messages avec un lien comme "Regarde ce que j'ai lu sur toi..." ou "Est-ce toi sur cette photo ?", mais ne vous faites pas attraper.

***Êtes-vous dans le doute?*** Contactez les autorités ou organisations compétentes par les voies officielles. Contactez votre supérieur hiérarchique si un paiement urgent doit être effectué à l'improviste sur ses instructions. En cas de doute, reportez toujours le paiement jusqu'à ce que vous ayez une certitude totale.

**Fraude à l'émotion**

Contrairement à la plupart des formes d'escroquerie en ligne, la stratégie des fraudeurs de l'émotion en ligne est quelque peu différente. Elle se manifeste comme suit :

- **Recherche :** Les escrocs vont d'abord faire les recherches nécessaires au préalable, afin d'avoir suffisamment d'informations de base sur le réseau social d'une personne. De cette manière, ils peuvent approcher la victime de manière très crédible. En fonction du phénomène, ils utiliseront la stratégie suivante :
    - **Fraude à la demande d'aide personnelle :** Les auteurs vérifieront à quoi ressemble l'environnement social de la victime potentielle. Combien d'enfants a-t-elle ? Est-ce qu'ils voyagent ? Quels sont les noms des petits-enfants et des animaux domestiques ? Ces informations seront utilisées lors du contact avec la victime, pour gagner sa confiance.
    - **Fraude à l'amitié:** Dans le cas de la fraude à l'amitié, les auteurs vont souvent plus loin. Ainsi, les gens investiront beaucoup plus de temps dans les chats en ligne avec la victime. Ceci dans le but de créer un lien de confiance avec la victime, étant donné que ces victimes sont connues pour en avoir particulièrement besoin.



Pour mieux protéger les citoyens contre ces formes d'escroquerie en ligne, on peut donner ces conseils de prévention spécifiques :

- Soyez toujours critique lorsque vous établissez des contacts en ligne et n'acceptez surtout pas de demandes de paiement sans avoir rencontré cette personne dans la vie réelle (en toute sécurité).
- Si une personne proche de vous demande en ligne un transfert d'argent urgent, un appel vidéo peut être recommandé comme moyen de contrôle (si le contact physique est impossible). Pour les paiements importants, ne virez jamais rien avant d'effectuer ce contrôle, quelle que soit l'authenticité de l'appel.
- En outre, pour éviter la fraude à la demande d'aide, il peut également être recommandé de poser une question dont la réponse n'est connue que par un contact étroit. Il faut veiller à ce que ces informations ne puissent pas être trouvées sur l'internet. C'est souvent difficile, étant donné la quantité d'informations qui circulent sur les médias sociaux.
- Au moindre doute, ne virez aucun somme.

## Réception d'un message suspect

De plus en plus de citoyens sont attentifs aux escroqueries en ligne et reconnaissent de nombreux faux messages. Dans ce cas, ils peuvent être encouragés à faire ce qui suit :

- **Envoyer le message à** suspect@safeonweb.be
- Ne cliquez pas sur les liens contenus dans le courrier électronique, mais consultez le site web via un moteur de recherche.
- Ne faites pas suivre le message à vos contacts, sauf par une capture d'écran pour sensibiliser les gens.
- Ne fournissez pas de données personnelles.
- Si un escroc se fait passer pour une organisation ou une entreprise, nous vous recommandons de prévenir cette organisation officielle. De cette façon, elle peut alerter ses clients.

## Pratiques locales inspirantes

Nous concluons cette boîte à inspiration par quelques pratiques qui peuvent être appliquées au niveau local. Certaines de ces initiatives ont depuis été lancées en Belgique également. Si vous avez lancé une autre bonne pratique qui ne figure pas dans la liste, n'hésitez pas à nous le faire savoir via consultancy@ibz.be .

*Les cyber-volontaires*

- Tous les groupes cibles peuvent être atteints, selon l'approche adoptée.
- Il s'agit d'utiliser des citoyens comme volontaires pour sensibiliser les citoyens vulnérables aux escroqueries en ligne. L'objectif est ici de sensibiliser les citoyens de manière accessible. Ce faisant, il est recommandé que chaque citoyen entre en ligne de compte comme cyber-volontaire. Ainsi, les informations peuvent être communiquées entre les citoyens de manière compréhensible.
- Les cyber-volontaires peuvent être déployés de plusieurs façons : l'écoute des victimes, des séances d'information dans les écoles et une sensibilisation proactive des personnes vulnérables de la région. Cependant, il est important ici qu'un cadre soit établi par l'autorité locale, dans lequel certains accords sont conclus. Ainsi, le cyber-volontaire sait quelles sont ses possibilités, mais l'autorité locale peut également agir si des abus devaient se produire.
- À cet égard, la formation au cyber-volontariat peut être dispensée par les autorités locales, une bonne coordination entre la zone de police et la commune étant fortement recommandée.
- En ce qui concerne le matériel de formation, on peut se référer en premier lieu au matériel déjà fourni par le CCB : Enseigner la cybersécurité | Centre pour la Cybersécurité Belgique (belgium.be) . En outre, vous pouvez également visiter le site web de Febelfin, votre guide . Vous pouvez également utiliser les informations fournies par la DG SP (www.besafe.be). Toutes ces informations peuvent être utilisées gratuitement lors des formations.
- Il est fortement recommandé de faire appel aux PLP opérant dans votre commune à cet égard. Cela peut servir de base pour développer le travail avec les cyber-volontaires. Si cela n'est toujours pas possible, il est possible de travailler avec des associations locales qui ont un intérêt à y participer.
- Encouragez également les jeunes à s'impliquer en tant que cyber-volontaires. Rendez cette fonction attrayante pour eux, en fonction des possibilités offertes au niveau local.
- Dans tout cela, il est important que l'autorité locale puisse garder la trace de ceux qui sont officiellement actifs en tant que cyber-volontaires. En effet, l'intention en agissant ainsi est simplement de sensibiliser les citoyens vulnérables. Les manipulations d'appareils ne sont donc pas à l'ordre du jour.

*Sachet de pain avec conseils de prévention*

- Adapté aux personnes âgées et aux personnes ayant des compétences numériques limitées.
- Atteindre un public cible plus âgé en matière de cyberprévention en ligne n'est pas facile. Des actions physiques, comme un sachet de pain contenant des conseils de prévention contre les escroqueries en ligne, sont souvent utiles. En s'associant avec des boulangers locaux, on peut mieux atteindre le public cible, renforcer l'économie locale et les entrepreneurs locaux peuvent également démontrer leur rôle social.
- Combinez de préférence cette action avec d'autres actions. De cette façon, un effet de sensibilisation plus important sera possible.

*Sensibilisation au marché*

- Adapté aux personnes âgées et aux personnes ayant des compétences numériques limitées.
- Un marché peut être une occasion idéale de toucher des personnes que les autorités locales ont du mal à atteindre par voie numérique.
- Ce faisant, il existe plusieurs façons d'agir pour sensibiliser les individus aux escroqueries en ligne. Dans cette optique, vous pouvez utiliser des dépliants ou brochures contenant des conseils sur la manière de reconnaître les tentatives d'escroquerie en ligne et sur ce qu'il faut faire si l'on en est victime.

*Séances d'information*

- Adapté aux personnes âgées et aux personnes ayant des compétences numériques limitées.
- Organisez une séance d'information sur les escroqueries en ligne dans votre collectivité locale. Dans de nombreux cas, cela permettra d'atteindre des personnes qui ont moins de compétences numériques. En même temps, cette bonne pratique assure la cohésion sociale dans la commune, car les habitants peuvent aussi apprendre à se connaître au cours de cette soirée.
- Fournir des informations accessibles qui ne nécessitent pas de connaissances techniques préalables particulières. Rendez-les accessibles à tous et aussi pratiques que possible. Ce faisant, osez également interagir avec le public. Cela vous fournira beaucoup d'informations et vous aidera à organiser les futures sessions d'information.
- En termes d'information, le matériel de formation fourni par le CCB peut être utilisé : Enseigner la cybersécurité | Centre pour la Cybersécurité Belgique (belgium.be) . En outre, vous pouvez également visiter le site web de Febelfin https://www.febelfin.be/fr . Vous pouvez également utiliser les informations fournies par la DG SP (www.besafe.be).

*Escape room*

- Adapté aux jeunes et aux personnes qui sont très familières avec l'internet.
- Pour aiguiser davantage leurs compétences numériques et les sensibiliser à l'impact que les risques en ligne peuvent avoir sur leur vie. Parallèlement, il convient de donner des conseils sur les points à surveiller dans le monde en ligne, sans être trop moralisateur. A cet égard, mettez toujours l'accent sur le rôle que les spectateurs (en ligne) peuvent jouer, faites porter la responsabilité sur le ou les auteurs et limitez autant que possible le blâme de la victime.

*Quiz*

- Tous les groupes cibles peuvent être atteints, selon l'approche adoptée.
- Préparez un quiz permettant d'affiner les compétences numériques. Cela permet de se former à la reconnaissance des e-mails frauduleux.
- Toutefois, il est également important de préciser les mesures que la personne concernée doit prendre face aux escrocs en ligne.

*Médias éducatifs*

- Adapté aux jeunes
- Il existe de plus en plus de jeux éducatifs sur le marché. Ces jeux peuvent également être très utiles pour sensibiliser et atteindre les jeunes, notamment en ce qui concerne les risques en ligne. En effet, ils semblent également être sensibles à diverses formes d'escroquerie et de violence en ligne.
    - Consultez également Hackshield et Space Shelter.
- Il est également possible de recourir à la tv éducative. Cette TV répond au style de vie des jeunes, mais en même temps avec un message éducatif.

*Etablir des collaborations locales*

- Dans un premier temps, il est recommandé de lancer un partenariat interne autour des cyberdéfis. Cela peut impliquer non seulement le service local de prévention et le service informatique, mais aussi, par exemple, le service de la jeunesse et les services sociaux.
    - Il est essentiel de prendre également en compte la sécurité interne des organisations gouvernementales locales. Étant donné le rôle important que jouent les collectivités locales dans la prestation de services et les données détenues sur les habitants, elles peuvent être la cible de cyberattaques. Les attaques réussies peuvent avoir un impact majeur sur les services, entraîner des coûts énormes et nuire à la réputation. Il est donc important d'élaborer un plan pour s'en prémunir de manière préventive. En outre, il est également préférable d'élaborer un plan d'urgence (cyber) qui indique clairement à chaque membre du personnel ce qu'il doit faire si l'administration locale est victime d'une cyberattaque. La vidéo suivante du CCB est fortement recommandée à cet égard : https://www.youtube.com/watch?v=ETtBwTZWsm4
    - Outre l'aspect très technique de la sécurité informatique, il s'agit également de sensibiliser l'ensemble du personnel. Il pourra ainsi apprendre à mieux reconnaître les messages suspects et contribuer à réduire le risque que les autorités locales soient victimes d'une cyberattaque.
      Plus d'infos : Cyberguide - Centre pour la Cybersécurité Belgique | (belgium.be)
    - En outre, des partenariats internes et externes peuvent être mis en place pour sensibiliser les citoyens.
- Tous les groupes cibles peuvent être atteints, selon l'association et l'approche.
- Chaque pouvoir local possède de nombreuses associations sur son territoire. Selon l'association, elles peuvent également être utilisées dans la cyberprévention. Cette mesure peut être combinée à l'une des bonnes pratiques susmentionnées.
    - Par exemple : session d'infos en collaboration avec le CPAS.
    - Par exemple, dans un club de jeunes, mettre l'accent de manière originale sur les risques en ligne, en lien avec un jeu.