FICHE MÉMOIRE
Arnaques en ligne

INTRODUCTION

Arnaques en ligne : reconnaître, éviter, réagir

Les arnaques en ligne se diversifient et deviennent de plus en plus sophistiquées.

- Apprenez à reconnaître les arnaques les plus courantes, comment les repérer grâce à des signes distinctifs, et adoptez les bonnes pratiques pour naviguer en toute sécurité.

SOMMAIRE

Skills to Connect

1 Reconnaître les principales arnaques

Voici les arnaques les plus fréquentes :

- **Phishing (hameçonnage)** : un faux email ou SMS vous pousse à cliquer sur un lien pour voler vos informations (mot de passe, numéro de carte...).

- **Spoofing (usurpation d’identité)** : un faux conseiller bancaire ou policier vous appelle ou vous écrit.

- **Fraude à l’achat** : vous commandez un objet sur un site qui n’enverra jamais rien.

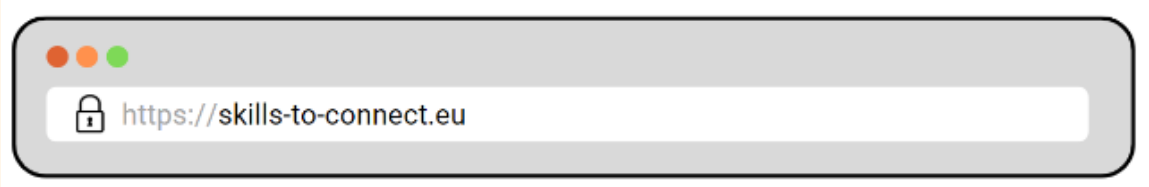
- **Fraude triangulaire** : vous achetez un produit volé sans le savoir.

2 Les signes à repérer

Toujours vérifier :

1. L'adresse du site qui doit toujours commencer :
   - la mention : https://
   - Un cadenas 🔒

✅ **Site sécurisé :**



🚫 **Site non-sécurisé**

2. L'apparence du message

3. L'adresse e-mail ou le numéro de l'expéditeur : Connaissez-vous cette adresse email ou l'expéditeur ?

2 Les signes à repérer

Voici les indices d’un message frauduleux :

🚫 **Méfiez-vous si** :

- On vous met la pression : « Votre compte sera bloqué sous 24h ! »
- On vous propose un cadeau ou une grosse réduction inattendue
- On vous demande vos codes, votre mot de passe ou numéro de carte
- Le message est écrit bizarrement :
  - Utilisation de deux langues (français-anglais)
  - Utilisation de caractères spéciaux
  - Fautes d’orthographe ou de syntaxe

Faux logo

le véritable logo de Google ressemble à ça : Google

Inhabituel

Mélange d'anglais et français

Pousse à action

Un lien frauduleux est dissimulé derrière le bouton

Message d'urgence :

Joue sur les émotions, le stress et sur un sentiment d'urgence pour vous pousser à l'action sans réfléchir

3 Se protéger facilement

Quelques réflexes à avoir :

1. **Protéger ses appareils :** Installez un antivirus sur vos appareils (ordinateur et tablette). Effectuez les mises à jour de vos appareils.
2. **Protéger ses comptes** : utilisez des mots de passe forts et différents, activez l'authentification à deux facteurs.
3. **Limiter les infos partagées :**

- Ne donnez pas vos données personnelles sur n'importe quel site et assurez-vous que le site est sécurisé et fiable (voir point 4 et 5).
- N'envoyez jamais votre numéro de carte, votre code PIN ou toute autre information bancaire à quiconque par e-mail.

4 Achats en ligne sécurisés

Quatres conseils :

1. **Achetez à des sources sûres** : privilégiez les marques et les boutiques dont vous avez l'habitude ou où vous avez déjà effectué vos achats, et vérifiez les notations des vendeurs privés sur les sites tels qu'Amazon ou Ebay.

2. **Si vous achetez quelque chose en ligne à un particulier sur un site de revente** (Marketplace, Ebay, Le bon coin, etc.) : N'envoyez pas l'argent au vendeur : proposez une remise en mains propres ou demandez à recevoir l'objet avant de payer.

3. **N’envoyez pas d’argent à quelqu’un que vous ne connaissez pas :** si quelqu’un vous aborde en ligne et demande de l’argent, demandez-vous si vous donneriez la même chose à un inconnu dans la rue.

4. **Évitez d’utiliser des sites d’achats en ligne qui ne demandent pas d’authentification complète et sauvegardez toujours les documents relatifs à vos achats en ligne :** Ils peuvent être utilisés comme preuve si vous ne recevez pas ce que vous avez payé pour ces biens.

5 Que faire si je suis victime d’une arnaque ou tentative d’arnaque ?

📌 **En cas de doute :** « J’ai reçu un mail suspect me demandant de cliquer sur un lien et d’envoyer mes coordonnées ou de les appeler»

Si je reçois un message suspect :

1. Ne pas cliquer sur le lien
2. Ne pas répondre au message
3. Ne pas transmettre le message à d'autres personnes
4. Ne pas appeler le numéro indiqué
5. Bloquer le mail en question et supprimer le message

📌Je suis victime d’une d'arnaque :

1. **Changez vos mots de passe immédiatement.**
2. **Contactez votre banque** si des données bancaires ont été partagées.
3. **Signalez l’arnaque :**
   - En Belgique : www.safeonweb.be
   - En France : www.internet-signalement.gouv.fr
   - En Europe : Site EU Victimes
4. **DÉPOSEZ PLAINTE :** Rendez vous au commissariat ou à la gendarmerie pour déposer plainte. Apportez toutes les preuves possibles : le numéro qui vous a contacté, les messages, emails ou captures d’écran liés à l’arnaque.

💡 Bon à savoir

Un conseiller bancaire **ne vous demandera jamais votre mot de passe, votre code PIN ou votre numéro de carte bancaire par téléphone ou par email**. Si quelqu'un vous les demande, il s'agit très probablement d'une arnaque.

Pour accéder à vos impôts, votre pension ou d'autres services publics en ligne en **Belgique**, il faut **toujours passer par la plateforme sécurisée CSAM ou l'application ITSME**. Vous ne recevrez jamais un email vous demandant de cliquer sur un lien pour voir votre déclaration d'impôt. Si vous recevez ce type de message, ne cliquez surtout pas : c'est une tentative de fraude.