# Le marché en ligne continue de croître, les cybercrimes également

Malheureusement, le nombre de cybercrimes dénoncés relatifs à la fraude lors des achats en ligne continue également d' **augmenter à une vitesse phénoménale**. Il y a tout le temps des marchands en ligne qui cessent leurs activités commerciales, mais personne ne se doute du fait qu'un bon nombre d'entre eux luttent contre les rejets de débit et doivent payer pour régler ce problème. Les consommateurs, d'autre part, sont obligés **de lutter pour distinguer les pubs du commerce électronique légitimes des fraudes sophistiquées**, cachées parmi des centaines d'offres apparemment non voulues et tentatives de hameçonnage.

Selon la Commission Fédérale de Commerce des États-Unis (FTC), les fraudes lors des achats en ligne impliquant **des produits destinés à la perte de poids** étaient la première catégorie de fraudes avec environ 5,1 millions de victimes. Un peu plus en bas de la liste, on trouve **la facturation non autorisée de services en lignes** (environ 1,9 millions) et **les fraudes de cartes de crédit** (environ 1,3 millions). Les fraudes passent inaperçues pour longtemps – si on ne s'en rend jamais compte – ; la détection se base d'abord sur des astuces proposées par des consommateurs vigilants qui reconnaissent certains comportements et donnent l'alerte.

Le FTC Consumer Sentinel Network Data Book a rapporté une **perte estimée de $450.000.000** suite aux fraudes lors des transferts monétaires d'un seul mois.

## Suivez votre intuition lorsqu'il s'agit d'achats en ligne

Imaginons la situation suivante : Dans la vie réelle, vous fieriez-vous à l'un de ces messieurs pour qu'il s'occupe de votre bébé pendant une journée ou de votre chien pendant votre absence, sans connaître toutes ses qualifications ? Nous espérons que non.

Revenons-en au monde numérique : Au regard de tout cela, pourquoi achèteriez-vous quelque chose en ligne ou utiliseriez-vous un service en ligne si le site web concerné propose *uniquement* le paiement par virement et **ne dispose pas d'adresse physique** ou d'un **numéro de téléphone opérationnel** que vous ne trouvez nulle part ? Gardez à l'esprit ce qui suit : Si une offre semble trop bonne pour être vraie, elle ne l'est probablement pas.

# 6 schémas de fraudes communs lors des achats en ligne

Jetons un coup d'oeil sur quelques pièges très communs lorsqu'il s'agit des paiements en ligne et voyons comment les reconnaitre.

- **Fraudes lors des ventes aux enchères sur Internet**

  Un consommateur paie un article qu'il vient de gagner sur un site dédié aux ventes aux enchères attractif, mais le vendeur soit envoie une contrefaçon ou un produit d'un valeur inférieur, soit ne livre rien du tout. Avec presque 500 rapports par semaine, les fraudes commises lors des ventes aux enchères représentent quelque 48% des rapports de fraude en ligne selon la FTC.

- **Hameçonnage à l'aide de bons d'achat et de promotions**

  Cette arnaque fonctionne de manière particulièrement efficace pendant la période de Noël. Les consommateurs reçoivent un e-mail qui semble provenir d'un revendeur autorisé. Malheureusement, les liens feignant de mener à la promotion vous mènent à une site web falsifié qui ressemble à l'original de façon trompeuse.

- **Fraudes dans la vente en ligne de voitures**

  Il y a des criminels qui essaient de se cacher derrière des noms d'entreprises renommées tels que eBay Motors Vehicle Purchase Protection (VPP), alors que VPP ne s'applique pas aux transactions hors d'eBay Motors et que les paiements par virement sont expressément interdits. Si vous êtes sûr de vouloir initier l'achat à distance d'un véhicule, veillez à ce que le vendeur ainsi que la possession de la voiture soient vraiment légitimes. *N'envoyez jamais de paiement par avance à une personne totalement inconnue.*

- **Fraudes lors des renouvellements de domaines**

  Les consommateurs reçoivent une facture falsifiée pour l'enregistrement ou le renouvellement d'un domaine qui correspond ou ressemble au leur.

- **Boutiques en ligne frauduleuses**

  La liste est interminable. Des pharmacies falsifiées, par exemple, proposent des médicaments à des prix très bas et/ou sans prescription. Tenez compte du fait que vous pourriez nuire à votre santé et perdre votre argent !

- **Les rejets de débit ou les fraudes « amicales »**

Après avoir reçu les biens achetés, un consommateur frauduleux demande un rejet de débit à la banque afin d'obtenir un remboursement. Le marchand est responsable, peu importe quelles mesures ont été prises au préalable pour vérifier la transaction.

## 11 astuces permettant d'éviter de perdre votre argent durement gagné à cause de fraudes lors de vos achats en ligne

1. **N'ouvrez jamais les e-mails non sollicités ou les pièces jointes provenant de sources inconnues**, surtout s'ils prétendent provenir de banques, services de paiements ou même d'organismes de poursuite légale tels que le FBI avec qui vous n'avez jamais été en contact avant. Veillez à *avoir un bon scanneur anti-malware muni de protection en temps réel actif*, qui analyse toutes les pièces jointes dès qu'elles sont ouvertes.

2. **Ne cliquez jamais sur les liens dans les e-mails non sollicités** et ne remplissez jamais de formulaires en ligne vous demandant des informations personnelles ou financières si ce formulaire est référencé ou joint au contenu d'un message de ce type. Veillez aux fautes d'orthographe difficiles à voir dans le lien et saisissez plutôt manuellement l'adresse dans la barre d'adresse de votre navigateur. Cherchez les informations contenus dans l'e-mail *directement* sur le site web.

3. **Lisez les clauses en petits caractères d'abord** avant de vous enregistrer et/ou de passer commande ou d'enchérir sur une offre. Décidez-vous pour un autre revendeur si les clauses en petits caractères vous inquiètent.

4. **N'envoyez jamais vos détails de compte en ligne**, votre numéro de sécurité sociale et/ou détails de votre carte de crédit dans un e-mail (non chiffré). Vous ne les mettriez pas sur le pare-brise de votre voiture tout en conduisant en ville, n'est-ce pas ? Malheureusement, il y a des boutiques en ligne qui s'inquiètent peu de votre vie privée, p. ex. en vous envoyant votre nom d'utilisateur et mot de passe que vous venez de créer en texte plein à titre de confirmation. Dans ce cas, nous vous conseillons d'*abandonner votre inscription avec effet immédiat*.

5. **Veillez à la présence d'un petit icône en forme de cadenas** en bas de votre navigateur ou à côté de « https » dans la barre d'adresse de celui-ci tout en accédant à des profiles, comptes d'utilisateur ou formulaires en ligne qui vous demandent de saisir des informations financières. Ceci ne vous garantit pas forcément la protection, mais c'est un bon début. Pour

d'autres informations vous aidant à reconnaître un site web sûr, veuillez continuer à lire «Dangers dans le réseau » dans notre base de connaissances.

6. **N'envoyez jamais d'argent par virement à une personne totalement inconnue**. Tenez compte du fait qu'un virement est comme un envoi d'argent dans une enveloppe simple. Utilisez plutôt votre carte de crédit ou un service de paiement fiable tel que Paypal qui vous propose un niveau de sécurité supplémentaire pour empêcher que votre compte bancaire ne tombe dans les mains d'escrocs. Même les entreprises dédiées aux transferts monétaires tels que Western Union et Moneygram vous encouragent expressément à ne *jamais* vous servir d'un transfert monétaire pour acheter un bien à une personne inconnue, et eux, ce sont des experts !

7. **Si vous vendez des biens en ligne**, en revanche, n'envoyez jamais les biens sans assurance. Si vous ne pouvez pas confirmer l'identité d'un acheteur, demandez toujours un paiement par avance. Ne remboursez personne vous ayant payé avec un chèque surpayé que vous avez reçu, mais pas encore encaissé – ce pourrait être l'arroseur arrosé !

8. **Suivez votre intuition** et/ou fiez-vous au savoir que vous trouvez sur Internet. Si une offre semble trop bonne, elle pourrait être falsifiée ou frauduleuse. Cherchez des statuts et conditions de l'entreprise sur Google, Bing ou Yahoo etc. Essayez également de chercher le nom de l'entreprise en vous servant de mots-clé tels que « fraude » ou « arnaque ».

9. **Vérifiez les factures de votre carte de crédit et vos relevés bancaires** de manière régulière afin de déceler tout chargement non autorisé le plus tôt possible.

10. **Utilisez un mot de passe différent, mais compliqué** pour chacun de vos comptes en ligne. Changez-les régulièrement, mais ne les sauvegardez pas dans votre boîte d'entrée.

11. **Protégez votre ordinateur** en vous servant d'un logiciel anti-virus qui propose plus de protection que les logiciels conventionnels. Les domaines légèrement modifiés ou comportant des caractères spéciaux pourraient d'abord ne pas sembler suspects. Malwarebytes, détecte la plupart des sites de hameçonnage et bloque toute tentative de connexion avec ceux-ci et vous protège ainsi contre le hameçonnage de la meilleure façon possible.