Finances

Achats

e-commerce

Santé

Tourisme

Véhicules

Immobilier
énergie

Justice

Centre Européen des Consommateurs France

Fraudes sur Internet

Comment éviter les pièges européens sur la toile ?

Protection des consommateurs en Europe
ECC-Net
Centre Européen des Consommateurs France

SOMMAIRE

Phishing, arnaque nigériane, fraude à la carte bancaire, abonnement caché, annuaire professionnel, spams... La cybercriminalité est sans limites et toujours novatrice. Afin d'éviter les pièges de la toile, le Centre Européen des Consommateurs France vous propose un tour d'horizon des fraudes européennes les plus courantes avec des conseils pour ne pas devenir les prochaines victimes.

Août 2017

ATTENTION

Le Centre Européen des Consommateurs France ne peut intervenir en cas de fraude. Mais n'hésitez pas à nous contacter pour tout renseignement sur votre vendeur ou sur vos démarches en cas de fraude avérée.

FAUSSES ANNONCES DE VOITURE À VENDRE

Vous trouvez la voiture de vos rêves à un prix défiant toute concurrence sur Internet. Pour réserver le véhicule, le vendeur vous demande de payer un acompte ou le prix total par virement bancaire sur un compte à l'étranger ou par mandat cash via des sociétés comme Western Union, MoneyGram. Une fois le transfert de fonds effectué, la vente n'a jamais lieu et le vendeur ne vous donne plus de nouvelles.

Conseils

- **Méfiez-vous des offres trop alléchantes** !
- **N'envoyez pas de montants importants vers l'étranger** sans avoir vu le véhicule.
- **Ne payez pas** la totalité du prix avant la livraison du véhicule.

Comment éviter les pièges ?

- Fuyez les vendeurs qui répondent de façon trop évasive à vos questions et qui exigent le paiement via un tiers de confiance non sécurisé.
- En cas de doute sur l'identité du vendeur, demandez une photocopie du passeport et des papiers du véhicule certifiée conformes.

Plus d'informations dans notre article « Achat d'un véhicule sur internet ».

PRODUIT DE GRANDE MARQUE À PRIX CASSÉS

Vous trouvez sur un site européen un produit de votre marque préférée vendue à un prix cassé. Mais une fois la commande réglée, le produit n'est jamais livré, il s'avère défectueux ou contrefait. Vous n'obtenez plus aucune nouvelle du vendeur.

Conseils

- Renseignez-vous auprès de votre banque et de l'établissement ayant délivré votre carte bancaire, si vous bénéficiez de **garanties** pour demander le **remboursement** de votre commande.
- Si la fraude est avérée, signalez les faits en France à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information

et de la Communication via le portail de signalement des contenus illicites de l'Internet.

- Vous pouvez aussi **signaler les faits à la marque pour les produits contrefaits** : détentrice des droits et brevets, elle pourra ensuite se retourner contre ces sites frauduleux.
- Si vous êtes victime de contrefaçon, vous pouvez **porter plainte** à la police ou la gendarmerie et saisir la douane ou les services de répression des fraudes de votre région.

Comment éviter le piège ?

Dans le moteur de recherche

- Si vous tapez le nom d'une grande marque dans un moteur de recherche, **méfiez-vous des sites référencés en bas de page ou non référencés sur la première page.** Les grandes marques ne manquent généralement pas de pratiquer un référencement efficace sur internet, souvent payant permettant de se hisser dans la première moitié de page voire en première position. Mais attention : **tous les sites figurant dans la première moitié de la page ne sont pas forcément officiels !** Certains faux sites peuvent être très bien référencés.
- Dans les résultats du moteur de recherche, **regardez bien la description** (appelée « snippet ») **située sous le lien du site affiché.** Le snippet du lien d'un site officiel présente généralement la marque en une ou deux phrases construites. **Le snippet d'un faux site se résume souvent à un enchaînement de noms de produits succédés d'expressions** telles que « pas cher », « livraison gratuite », « économie », « femme », « homme » ou encore un pourcentage de réduction, correspondant purement à un ensemble de mots-clés que taperaient les consommateurs ciblés sur un moteur de recherche.

Sur le site

- Vérifiez qui a enregistré le site et à partir de quel pays via WHOIS, DENIC (pour les noms de domaine en .de), AFNIC (pour les noms de domaine en .fr).

- **Comparez les prix pratiqués avec la boutique officielle de la marque.** Méfiez-vous des prix trop bas ou mentionnant une réduction importante. Vérifiez que le site dispose de mentions légales faisant apparaître les coordonnées complètes du vendeur et de conditions générales de vente.
- **Comparez le logo de la marque** avec celui qui est affiché sur le site en question.
- **Lisez attentivement les offres, conditions générales… sur le site**. Si elles sont rédigées dans un français approximatif, il peut s'agir d'un faux site, les véritables titulaires de marques ou revendeurs agréés étant assez attentifs à l'utilisation de la langue française.
- Enfin, **faîtes attention aux modes de paiement proposés** : préférez toujours des modes de paiement vous permettant de voir réellement le produit avant de payer. Le plus souvent un site commercialisant de la contrefaçon, exigera un paiement à l'avance. **Évitez les transferts d'argent en liquide par mandat cash ou postal**, sans garantie.

Auprès du vendeur officiel

Renseignez-vous auprès du vendeur officiel de la marque afin de vérifier si le site fait partie de leurs revendeurs autorisés et signalez-lui tout vendeur indésirable. Certains produits de luxe, à forte spécificité ou de haute technologie, sont en effet commercialisés uniquement dans un réseau de distribution restreint. Ceux-ci ne pourront alors pas être valablement vendus neufs sur un site internet tiers et des produits proposés dans ces conditions seront forcément des contrefaçons, peu importe les allégations dudit site. Les entreprises sujettes à de fortes copies de leurs produits tiennent parfois sur leur site internet la liste des seuls vendeurs agréés.

Plus d'informations dans notre article « Contrefaçons » et « Achats de vêtements de grande marque à prix mini ».

ACHAT BLOQUÉ EN DOUANE

Vous effectuez un achat en ligne sur un site présenté comme européen mais votre commande, provenant d'un pays hors UE, **se retrouve bloquée en douane.** Des frais supplémentaires vous sont demandés ne garantissant pas la livraison des articles qui sont souvent issus de la contrefaçon.

Conseils

- **Ne payez pas les frais supplémentaires**.
- Demandez par écrit **l'annulation** de la commande et le **remboursement** des sommes versées au vendeur.

Comment éviter le piège ?

- Pour vous assurer de l'origine du produit commandé, vérifiez l'**identité et les coordonnées de votre vendeur** dans l'onglet « mentions légales » du site marchand.
- À défaut, recherchez ces informations via des sites comme WHOIS, DENIC, AFNIC (pour les noms de domaine en .fr).

ABONNEMENTS CACHÉS

Une publicité, un sondage sur Internet, propose de vous envoyer un cadeau gratuitement, un échantillon à 1€, etc. Seuls les frais de port sont à votre charge, s'élevant généralement de 4 à 5€. Pourtant quelques semaines plus tard, vous découvrez que votre compte bancaire a été débité d'une somme bien plus importante que celle annoncée lors de la commande par le site basé dans un pays de l'UE. Sans avoir été clairement informé sur le prix total à payer ainsi que sur le service souscrit, en acceptant l'échantillon offert, vous avez souscrit un abonnement avec des prélèvements tous les mois pouvant aller de 70 à 150 € ou plus.

Conseils

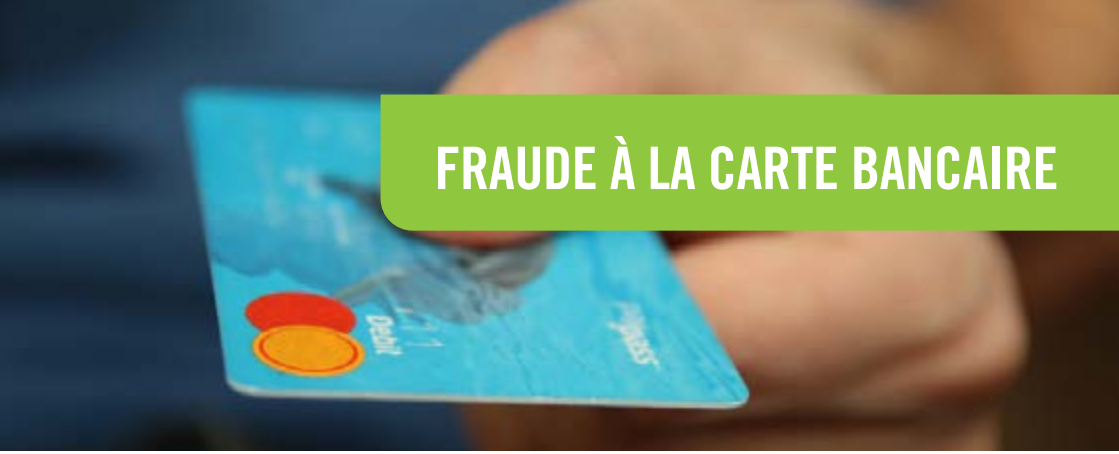
- Contactez le professionnel par lettre recommandée avec accusé de réception ou par courriel, pour demander la **résiliation** de l'abonnement et l'**annulation des nouvelles livraisons futures.**
- Si vous estimez ne pas avoir été suffisamment informé du caractère payant de cet abonnement, contestez sa validité. N'oubliez pas de **demander le remboursement** des sommes versées.
- Si vous venez de passer commande, **faites jouer votre droit de rétractation de 14 jours.** Renvoyez les colis reçus à l'adresse mentionnée sur le site ou précisée ultérieurement par la société.

- **Faites opposition aux futurs prélèvements** en contactant votre banque.
- En cas de litige avec un professionnel basé dans l'UE, en Islande ou en Norvège, n'hésitez pas à **contacter le Centre Européen des Consommateurs France**.

Comment éviter le piège ?

- **Méfiez-vous des offres trop alléchantes ou gratuites** avec pour seule contrepartie en apparence, le paiement des frais de livraison souvent modiques.
- Lors de votre inscription, vérifiez qu´**aucune case n´est pré-cochée.**
- Lorsqu'une fenêtre pop-up apparaît sur votre écran, ne cliquez pas sur les boutons qui vous sont proposés : votre clic peut signifier votre consentement à un abonnement payant.
- **Lisez attentivement les conditions générales de vente** et gardez-en une copie.

Plus d'informations dans notre article « Les abonnements cachés sur internet ».



FRAUDE À LA CARTE BANCAIRE

Vous constatez sur votre relevé de compte des paiements vers un professionnel basé dans un autre pays. Si vous n'êtes pas à l'origine de ces paiements, c'est que les numéros de votre carte bancaire ont été piratés.

Conseils

- **Consultez régulièrement vos relevés de compte.**
- **Faites opposition à votre carte bancaire.**
- Si les données de votre carte bancaire ont été utilisées à votre insu, votre responsabilité ne peut, en principe, être engagée. **Contestez par écrit les débits frauduleux à votre banque** dans les meilleurs délais et au plus tard dans les 13 mois pour un débit dans l'UE, le Lichtenstein, l'Islande et la Norvège ou dans les 70 jours pour un paiement frauduleux hors Espace économique européen. Après la réception de votre lettre recommandée, l'établissement bancaire doit vous recréditer immédiatement les sommes litigieuses. Plus d'informations sur notre article « Moyen de paiement : carte bancaire ».
- Vous pouvez également porter plainte au commissariat le plus proche.

Comment éviter le piège ?

Avant tout paiement par carte sur Internet, regardez si le site de paiement est sécurisé. **Un cadenas et le sigle « https »** (au lieu de «http») doit s'afficher dans la barre d'adresse du site, ce qui permet des envois cryptés.

FAUX SITES DE PAIEMENT SÉCURISÉ

Le cybermarchand basé dans un autre pays vous propose de payer votre commande via un système de paiement sécurisé. Vous vous laissez rediriger vers un soi-disant site de paiement sécurisé, qui ressemble aux sites de paiements connus : logos, conditions d'utilisation et mentions légales. Mais ce faux site appartient en fait au vendeur et non à une société financière, vous ne recevez pas votre commande et vous n'obtenez pas le remboursement des sommes versées.

Conseils

Si vous avez déjà payé et que vous ne recevez pas de courriel de confirmation de paiement, il s'agit certainement d'un faux site. Tentez une action en remboursement auprès de votre banque.

ATTENTION

Attention aux faux sites de transport ! Un soi-disant vendeur peut vous proposer de passer par un tiers de « confiance » pour le paiement ET la livraison du bien acheté. Mais une fois le paiement réalisé, vous resterez sans nouvelles de votre commande et sans possibilités de vous faire rembourser.

Comment éviter le piège ?

- Lorsque le site marchand vous redirige vers un site de paiement sécurisé, **vérifiez que cette page est bien sécurisée.** La page devra obligatoirement comporter un petit cadenas fermé et l'adresse du site devra commencer par https.
- Vérifiez l'adresse Internet du site sur lequel vous avez été redirigé via WHOIS, DENIC, AFNIC (pour les noms de domaine en .fr).
- Si le site sur lequel le vendeur vous redirige ne vous offre pas la possibilité de créer votre compte, il ne s'agira pas d'un paiement sécurisé mais d'un simple paiement par carte.

Plus d'informations dans notre article « Paiements en ligne ».

CONCOURS / LOTERIES

Une société vous adresse une promesse de gain et réclame le paiement de divers frais pour le recevoir.

Conseils

Si vous n'avez pas participé à ce concours, vous ne pouvez être le grand gagnant : ne répondez pas à la proposition !

Comment éviter le piège ?

- Lisez attentivement le courrier reçu.
- Méfiez-vous des offres qui conditionnent la réception du gain par une commande, même d'un montant minime.

Plus d'informations dans notre article « Se protéger contre les publicités non-sollicitées en Europe »

PHISHING

Vous recevez un courriel censé provenir de votre banque, de votre assurance ou d'un organisme administratif vous demandant de confirmer vos coordonnées bancaires ou d'envoyer des informations personnelles sous prétexte que vos données ont été perdues ou qu'une actualisation de votre dossier est nécessaire.

Conseils

- Vérifiez auprès de l'organisme si le courriel provient bien de ses services.
- N'envoyez jamais vos coordonnées bancaires via Internet ou courriel.

Comment éviter le piège ?

- **Vérifiez l'adresse courriel de l'émetteur.** Une banque ou toute autre administration n'utilise en principe pas de messagerie gratuite (ex : gmail, hotmail, etc).
- **Soyez vigilant face aux courriels mal orthographiés ou rédigés dans un français approximatif.**
- **Consultez le site internet de la société qui est censé vous avoir contacté.** Certaines publient des informations concernant les cas de phishing typiques les concernant ou encore un modèle de leurs e-mails pour le comparer à celui reçu. Certaines proposent également un interlocuteur

à laquelle vous pouvez faire parvenir une copie du faux e-mail.

- Si le lien d'un site figure dans l'e-mail suspect, vous pouvez également vous rendre sur le site www.phishing-initiative.com. Par le biais de ce site, vous pouvez renseigner le nom du site en question et solliciter l'avis d'un expert qui vérifiera s'il s'agit réellement d'un site de phishing, 24h/24 et 7j/7.
- Méfiez-vous également des appels de soi-disant conseillers bancaires, qui, au motif d'opérations inhabituelles sur votre compte bancaire, vous demande de confirmer vos coordonnées bancaires ou votre numéro de carte par téléphone.

Plus d'informations sur la protection de vos données personnelles sur notre site internet.

PIRATAGE DE COMPTE EMAIL OU DE PROFIL INTERNET

Vos contacts reçoivent un email provenant de votre adresse leur demandant une aide financière ou diffusant des informations publicitaires. Votre profil sur un réseau social est modifié ou envoie des messages sans votre accord.

Conseils

Si vous constatez une connexion sur votre compte par un inconnu ou la création d'un compte à partir de votre adresse e-mail, signalez-le directement auprès du réseau social en question et modifiez le mot de passe de votre boîte mail.

Comment éviter le piège ?

- **Choisissez un bon mot de passe** : minimum 8 caractères, avec des chiffres, des lettres majuscules, des lettres minuscules et des symboles, pas un mot du dictionnaire, pas d'information personnelle (date de naissance par exemple), différent pour chaque application, fichier et système utilisé. Pensez à le changer régulièrement (tous les 3 ou 6 mois selon son utilité).
- **Sécurisez votre connexion Internet.**

Plus d'informations dans notre rubrique « Protéger mes données ».

ARNAQUE NIGÉRIANE

Une personne demande votre aide pour effectuer un transfert d'argent pour des raisons soi-disant d'ordre diplomatique ou familial. En échange, elle vous offre un pourcentage sur la somme transférée. Si vous acceptez, vous devrez avancer de l'argent censé couvrir divers frais avant le transfert qui n'aura finalement jamais lieu.

Conseils

Ne répondez jamais à ces courriels. N'envoyez pas non plus d'accusé de réception.

Comment éviter le piège ?

- Supprimez systématiquement ces messages non désirés.
- Plaçez-les dans le dossier « courrier indésirable » de votre messagerie.

Plus d'informations dans notre article sur les SPAMS

AUTRES SPAMS

Vous recevez des emails vantant les mérites d'un produit ou d'un service ou appelant aux dons pour diverses causes. Ces messages non sollicités proviennent d'expéditeurs inconnus.

Conseils

- Supprimez systématiquement ces messages non désirés.
- Plaçez-les dans le dossier « courrier indésirable » de votre messagerie.
- N'ouvrez jamais les pièces jointes et ne cliquez jamais sur les liens affichés.

Comment les éviter ?

- Utilisez une autre adresse email pour commander en ligne.
- Installez un filtre anti-spam.

Plus d'informations dans notre article sur les SPAMS

ANNUAIRES PROFESSIONNELS

Vous recevez une proposition d'insertion ou une demande de vérification de vos coordonnées dans des annuaires professionnels ou des registres spécialisés. Une fois rempli et signé, vous apprenez que le formulaire, avec entête et logo soi-disant officiels, renferme une obligation de payer plusieurs centaines d'euros pendant quelques années.

Conseil

- Si vous avez signé et renvoyé le formulaire, demandez expressément l'annulation du contrat pour dol ou erreur,
- Déposez une plainte auprès du parquet compétent et prenez les conseils d'un avocat en cas d'action de la société d'annuaire professionnel devant un tribunal européen.
- Si l'annuaire est situé en France, adressez-vous au représentant local de la Direction générale de la répression des fraudes.
- Alertez votre chambre des métiers, de commerce ou d'agriculture, ordre professionnel ou autre organisme d'affiliation.

Comment éviter le piège ?

- **Informez vos employés ou bénévoles** en charge du traitement du courrier de ce type d'escroquerie.
- Vérifiez l'identité et le logo de la société et comparez-les avec des sites officiels.
- **Recherchez le prix caché** dans les conditions générales écrites généralement en petits caractères en bas ou au verso du formulaire.

Protection des consommateurs en Europe

ECC-Net

Centre Européen des Consommateurs France

Membre du réseau des Centres Européens des Consommateurs (ECC-Net)

Nous...

- vous informons sur vos droits de consommateur européen,
- vous assistons en cas de litige avec un professionnel établi dans un pays de l'Union européenne, en Islande ou en Norvège.

Ouverture des bureaux au public du mardi au jeudi,
de 9h à 12h et de 13h à 17h.

Tel : 0049 7851/99 148-0

0 820 200 999 Service 0,12 € / min + prix appel

E-Mail : info@cec-zev.eu

Bahnhofsplatz 3
77694 Kehl
Allemagne

www.europe-consommateurs.eu

Cofinancé par l'Union européenne

Centre Européen de la Consommation
Zentrum für Europäischen Verbraucherschutz e.V.
www.cec-zev.eu