Achats et paiement en ligne
sur PC, smartphone et tablette

Vérifier la réputation du site internet

Privilégiez les grands sites connus comme la Fnac, Darty, Boulanger, Amazon …. (un site ayant pignon sur rue est préférable)

Pour être sûr que le site sur lequel vous souhaitez acheter un produit est fiable, la Direction générale de la concurrence, de la consommation et de la répression des fraudes(DGCCRF) recommande « d'entrer le nom du site ou du produit sur un moteur de recherche, éventuellement associé avec le terme arnaque ». Dans les résultats de la recherche, vous pourrez vérifier si d'autres internautes ont déjà eu des mauvaises expériences avec le vendeur.

Vérifier les mentions légales (en bas de page)

Les sites internet ont l'obligation de publier les mentions légales: il vous est ainsi possible de vérifier le nom, la dénomination sociale, l'adresse, les contacts, etc.

Être vigilant face à une offre trop alléchante

Enfin, faites attention aux offres trop alléchantes. Elles cachent souvent des arnaques. Vérifiez attentivement le descriptif, « ne vous contentez pas de la photo ! », précise la DGCCRF.

Ne pas se fier uniquement aux avis des consommateurs

Les avis des consommateurs ne sont pas toujours fiables. Qu'il s'agisse de faux avis positifs postés par le professionnel, ou par son agence de communication, ou d'avis négatifs rédigés par un concurrent, les faux commentaires sur les sites en ligne trompent le consommateur et faussent la concurrence, même si la pratique des faux commentaires est interdite en France.

Préférer un site européen ou français

Il est conseillé de choisir un site français ou européen, afin de vous garantir des droits (comme le droit de rétractation par exemple) que ne garantissent pas les sites installés hors de l'Union Européenne.

Cypiée 20 route Napoléon 38119 Pierre-Châtel
Tel : 04 76 30 15 78 – 06 95 35 03 58
animateurcypiee@gmail.com www:cypiee.fr

Être vigilant lors du paiement

Avant de payer, le vendeur doit vous permettre de vérifier le détail de votre commande et son prix total. La DGCCRF explique : « Le consentement se caractérise par un double clic :

- le 1er clic permet de vérifier la nature et la composition de la commande
- le 2ème clic permet de confirmer définitivement la commande. »

Au moment de payer, vérifiez que le site sur lequel vous êtes en train de payer est bien sécurisé. Sur certains sites, l'Url de la page http:// devient **https://**, avec l'ajout du s pour « Secure », un **cadenas fermé** peut aussi apparaître dans la fenêtre de votre navigateur. La DGCCRF précise que : **« le vendeur doit vous confirmer que votre page est bien sécurisée dans une fenêtre de dialogue avant le début de toute transaction. »**

Pour plus de sécurité lors du paiement en ligne, il est aussi recommandé de choisir une double précaution auprès de votre banque pour effectuer votre achat. Il s'agit par exemple de confirmer votre achat grâce à un **code reçu par SMS.**

La CNIL (Commission nationale de l'informatique et des libertés) déconseille également de laisser certaines applications et certains navigateurs internet enregistrer vos coordonnées bancaires pour ne pas avoir à les retaper ultérieurement. Ces terminaux ne garantissent pas toujours la sécurité de données bancaires.

Après avoir réglé votre achat, vérifiez que le montant débité sur votre compte correspond bien à la commande effectuée.

Paiement en ligne : 6 conseils pour éviter les risques de piratage

La France compte plus de 200 000 sites marchands sur internet, un nombre qui a été multiplié par 10 en dix ans. Si dans une grande majorité de cas les achats sur internet se déroulent sans incident, certains fraudeurs profitent des achats en ligne pour pirater les comptes bancaires des consommateurs et réaliser à leur insu des opérations frauduleuses. Voici nos conseils pour réaliser vos achats en toute sécurité.

1. Choisissez la double sécurité avec votre banque

Deux précautions valant mieux qu'une, utilisez les doubles sécurités de paiement proposées désormais par la plupart des banques.

Outre le traditionnel cryptogramme visuel (généralement un code à trois chiffres situé derrière votre carte), il vous est possible de valider votre paiement en ligne par une seconde étape. Généralement en rentrant un code qui est envoyé par votre banque juste après le paiement.

Il s'agit la plupart du temps d'un **code envoyé par SMS** que vous devez renseigner pour confirmer votre commande.

2. Vérifiez que la page est bien sécurisée

- **Il est vivement recommandé de faire vos achats sur un site web disposant d'une sécurité « https »** : en effet, il existe 2 types de sites internet. Ceux dont l'adresse commence par « **http://** » et ceux dont l'adresse commence par « **https://** ». Évitez de faire vos achats sur les sites en « http:// » et ne créez par un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires ...) peuvent être interceptées par des tiers (attention, cette condition est nécessaire, mais pas suffisante).
- **Par ailleurs, ne partagez jamais des informations personnelles (mot de passe par exemple)** : aucun site fiable ne vous demande ce type d'informations.

3. Prenez garde aux sites inconnus et aux offres trop alléchantes

Certaines offres sont parfois trop alléchantes pour être vraies.

- Ne craquez pas sur de prétendues bonnes affaires sans avoir vérifié la réputation du site auparavant.
- Lisez les notes et avis de consommateurs.
- Méfiez-vous des sites qui proposent un prix nettement plus bas que leurs concurrents.

4. Évitez d'enregistrer vos coordonnées bancaires

Réfléchissez à deux fois avant de garder en mémoire votre numéro de carte sur votre téléphone ou votre ordinateur. Certaines applications et certains navigateurs internet vous proposent d'enregistrer vos coordonnées pour ne pas avoir à les retaper ultérieurement. Une méthode déconseillée par la CNIL : « ces terminaux ne sont pas nécessairement conçus pour garantir une sécurité optimale des données bancaires ».

5. Méfiez-vous des réseaux WiFi publics

Pas de précipitation pour faire vos achats.

- Si vous êtes connecté à un WiFi public, dans un café, un hôtel ou une gare par exemple, **mieux vaut ne pas rentrer votre numéro de carte**. En effet, la Cnil met en garde : « Un éventuel pirate peut saisir l'occasion d'un WiFi mal chiffré pour (...) intercepter certaines de vos données ».
- Attendez d'être plus à l'abri, sur un réseau privé.

6. Assurez votre sécurité numérique globale

Au-delà même de la nécessaire vigilance dont vous devez faire preuve au moment de vos achats en ligne, être vigilant concernant votre sécurité numérique au quotidien vous permettra de sécuriser d'autant plus vos paiements. À ce titre, le respect de quelques conseils de base peut être utile :

- **Sécurisez votre terminal informatique** : mettez à jour régulièrement vos équipements, utilisez un anti-virus et un pare-feu, sécurisez votre accès au wifi, etc.
- **Consultez régulièrement votre compte bancaire en ligne** : afin de vérifier qu'aucune transaction douteuse n'a été réalisée.
- **Sécurisez vos mots de passe** : variez-les, réservez chacun d'entre eux à un usage unique et créez des mots de passe qui remplissent toutes les conditions de sécurité.
- **Utilisez votre messagerie de façon sécurisée** : lisez attentivement les informations contenues dans les courriels, ne cliquez pas sur les pièces jointes ou sur les liens qui paraissent douteux, etc.

7. En cas d'incident, contactez d'abord votre banque

- Si vous constatez avoir été piraté suite à un achat en ligne, **contactez tout d'abord votre banque** pour faire opposition sur votre carte bancaire et pour ensuite demander le remboursement des opérations frauduleuses ou demander l’attribution d’une nouvelle carte bancaire.
- L'opposition sur votre carte bancaire peut également être réalisée via l**e service interbancaire d'opposition à carte bancaire** 0 892 705 705 (ouvert 7 jours/7 et 24h/24), numéro surtaxé : coût d'un appel vers un numéro fixe + 0,34 € TTC/min, depuis un téléphone fixe ou mobile
- Vous pouvez ensuite **signaler ce piratage sur Perceval**, la plateforme de signalement des fraudes à la carte bancaire.