

Ce site utilise et partage avec des tiers (partenaires ou prestataires) des cookies et autres traceurs à des fins de statistiques et de mesure d'audience, de partage de contenu sur les réseaux sociaux et d'utilisation d'outils de visualisation multimédia.

Le dépôt de ces cookies est soumis à l'obtention de votre consentement préalable à l'exception de certains cookies nécessaires au fonctionnement du site et des cookies de mesures d'audience pouvant être regardés comme exempts de consentement. Vous pouvez paramétrer votre choix, finalité par finalité, en cliquant sur « Paramétrer » et modifier votre choix à tout moment lors de votre navigation sur le site en cliquant sur l'onglet « Gérer les cookies » (accessible sur le site, en bas de page). Pour plus d'informations, [voir notre politique Cookies](#).

[ACCEPTER](#)

ACHATS DE NOËL EN LIGNE : NOS CONSEILS POUR SÉCURISER VOS ACHATS

Date de publication : 10/12/2021 - Commerce/services



Simple et rapide, des prix parfois plus attractifs : la vente en ligne offre de nombreux atouts et favorise les achats, surtout en cette période de Noël.

Mais attention aux risques de fraudes et d'arnaques. La vigilance s'impose donc pour éviter de tomber dans certains pièges.

L'Institut national de la consommation vous informe et vous donne des conseils pour réaliser vos achats en ligne en toute sérénité.

LES 7 POINTS A VERIFIER AVANT D'ACHETER SUR INTERNET

QUE FAIRE SI VOUS AVEZ ETE VICTIME D'UNE ARNAQUE EN CAS D'ACHAT SUR INTERNET ?

LES 7 POINTS A VERIFIER AVANT D'ACHETER SUR INTERNET

Le risque de cybercriminalité est important, d'autant plus, pendant la période de Noël : fausses promotions, faux sites web de marchands officiels, hameçonnage par SMS, téléphone ou courriel, faux transporteur?

Le consommateur est souvent pressé, il souhaite avoir le dernier jouet à la mode, il craint le risque de pénurie de jouets relayé par les médias, il veut être livré à temps pour déposer le cadeau sous le sapin...

Autant d'éléments qui peuvent l'inciter à se précipiter et à être moins vigilant. Les cyber-escrocs en profitent donc pour lancer de nouveaux pièges.

> Pour en savoir plus, visionnez les vidéos Consomag "[Comment se protéger contre les cyber-escrocs](#)" réalisées avec Cybermalveillance.gouv.fr.

1 - Vérifiez que le site marchand est sécurisé

Soyez toujours prudent lors de la saisie de vos données bancaires.

Vérifiez notamment que le site marchand sur lequel vous naviguez est sûr. Pour cela, vérifiez son adresse dans la barre de navigation : celle-ci doit toujours commencer par **https://**, le **s** indiquant que la communication avec le site est sécurisée, et donc que les informations qui transitent ne sont pas piratables. Un petit cadenas précède souvent l'adresse et confirme que vous pouvez naviguer en toute sécurité.

Toutefois, la mention "**https**" ne suffit pas à garantir la fiabilité d'un site.

2 - Vérifiez la e-réputation du site et la fiabilité du vendeur

Avant toute commande, vérifiez que le site est bien rattaché à une entreprise.

Vérifiez notamment que figurent, souvent en bas de page :

- les conditions générales de vente (CGU) : elles indiquent notamment les conditions de vente, de livraison, de garantie et de retour des produits,
- les mentions légales : elles vous disent qui se trouve derrière le site web, ce qui vous permet notamment de savoir où se situe l'entreprise.

La e-réputation peut être vérifiée en entrant le nom du site ou du produit sur un moteur de recherche, éventuellement associé avec le terme "arnaque".

> Pour en savoir plus, consultez l'article "[Vérifier la fiabilité du vendeur](#)" sur le site du Centre Européen des consommateurs France (CEC).

En savoir plus

Il est recommandé de privilégier des achats sur des sites d'entreprises françaises ou de l'Union européenne. En achetant sur des plates-formes d'achat européennes, vous êtes mieux protégé en cas de litige.

3 - Vérifiez les avis des acheteurs

Vous pouvez vérifier les avis des acheteurs mais méfiez-vous tout de même des avis dithyrambiques ! Trop beaux pour être vrais !

> Pour en savoir plus, consultez l'article "[Peut-on faire confiance aux avis en ligne ?](#)" du site [economie.gouv.fr](#).

4 - Faites attention au dropshipping

Cette méthode commerciale consiste à vendre en ligne des produits alors que le vendeur n'a pas de stock. Les produits commandés seront directement envoyés par le fabricant au consommateur. Mais les délais de livraison sont souvent plus longs, ce qui peut être problématique au moment de Noël. Les cadeaux ne seront pas à temps sous le

sapin !

> Pour en savoir plus, consultez l'article "[e-commerce et dropshipping : pourquoi s'en méfier](#)" sur le site du Centre européen des Consommateurs France (CEC).

5 - Pensez à télécharger un anti-virus sur votre ordinateur et votre smartphone

Pensez à protéger les appareils avec lesquels vous allez effectuer vos achats en ligne, surtout les appareils mobiles (ordinateur portable, smartphone, tablette...) qui peuvent être perdus ou volés.

> Pour en savoir plus, consultez l'article "[Protéger ses appareils mobiles](#)" de [Cybermalveillance.gouv.fr](#).

6 - Faites attention aux modes de paiement proposés sur les sites d'occasion

Si vous achetez sur des sites d'occasion ou de vente entre particuliers, faites attention aux modes de paiement.

Privilégiez la remise en main propre contre un paiement en espèces, ou utilisez les systèmes de paiement sécurisés proposés par les plateformes de vente.

Et veillez à bien rester sur ces plateformes. Si le prétendu vendeur vous propose d'en sortir, cherchez un autre vendeur.

7 - Faites attention aux arnaques

• L'hameçonnage ou phishing

Attention aux faux sites qui imitent les sites officiels des commerçants. Il est préférable de se connecter directement en tapant le nom du site voulu dans la barre de recherche. Certains escrocs dupliquent "à l'identique" les sites web de commerçants.

Attention aussi aux mails reçus avec des liens qui peuvent être source de phishing ou d'hameçonnage.

> Pour en savoir plus, visionnez la vidéo Consomag "[Comment reconnaître un message de phishing](#)" et consultez notre dossier "[Comment se protéger contre les cyber-escrocs](#)" avec [Cybermalveillance.gouv.fr](#).

• L'arnaque au colis ou fausse commande

?En cette période, on attend souvent la livraison d'un colis. L'arnaque au colis consiste à envoyer un SMS de livraison de colis. Vous pensez que ce sms vous est destiné car vous avez effectué une commande, mais en réalité il s'agit d'un SMS envoyé de manière aléatoire par des escrocs et l'objectif est que vous transmettiez vos identifiants de connexion à vos comptes bancaires.

Dans le sms de réception du colis, il y a un lien. En cliquant sur ce lien, au lieu d'accéder au site du transporteur du colis, vous devez télécharger une application qui vous permet de suivre la livraison. Cette application s'installe automatiquement sur votre smartphone sans que vous passiez par Google Play ou Apple Play.

Lors de l'installation de l'application, vous autorisez souvent l'accès à vos données personnelles (localisation, contacts, SMS...). Sachez que vous pouvez refuser !

Par la suite, lorsque vous vous connectez à votre application bancaire, le logiciel malveillant récupère alors les identifiants bancaires que vous tapez, ainsi que le SMS de validation envoyé par la banque.

Les escrocs peuvent alors accéder à vos comptes bancaires.

> Pour en savoir plus, consultez l'article "[L'escroquerie à la fausse commande](#)" sur le site [Cybermalveillance.gouv.fr](#).

Il existait déjà des sms ou mails vous indiquant que vous deviez régler des frais d'affranchissement d'un colis. Pour cela, vous communiquiez vos numéros de carte bancaire qui étaient récupérés par les escrocs.

Notre conseil

Ne cliquez pas sur les liens reçus par SMS ou par mail.

QUE FAIRE SI VOUS AVEZ ETE VICTIME D'UNE ARNAQUE EN CAS D'ACHAT SUR INTERNET ?

En cas de problème, vous pouvez effectuer un signalement sur la plateforme publique [SignalConso.gouv.fr](https://signalconso.gouv.fr) afin d'alerter les professionnels de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

Vous pouvez également prendre contact avec une association de consommateurs qui pourra vous apporter des informations et vous aider dans vos démarches.

> Consultez l'article "[Quels sont les recours en cas d'arnaque sur internet ?](https://www.economie.gouv.fr/actualites/Quels_sont_les_recours_en_cas_d_arnaque_sur_internet_?lang=fr)" sur le site [economie.gouv.fr](https://www.economie.gouv.fr).

Corinne Lamoussière-Pouvreau,
Juriste à l'Institut national de la consommation

URL source: <https://www.inc-conso.fr/content/achats-de-noel-en-ligne-nos-conseils-pour-securiser-vos-achats>