

# Paiement en ligne : 7 conseils pour éviter les risques de piratage

Par **Bercy Infos** < <https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous> >, le 16/01/2023 - **Achats sur internet** LECTURE : 4 MINUTES

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.

\* Source : **Fédération du e-commerce et de la vente à distance (Fevad)** < <https://www.fevad.com/> >

## 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. Parfois également, vous devez ouvrir l'application de votre banque sur votre smartphone pour valider la transaction.

### Connaissez-vous les cartes bancaires virtuelles ?

Certaines banques proposent un service - généralement gratuit - de « **carte bancaire virtuelle** » ou « **e-carte bleue** » pour les achats en ligne. Le principe est simple : afin de réaliser un achat en ligne, la banque met à votre disposition une carte bancaire dématérialisée que vous n'utilisez que pour cet achat. Comme une carte classique, elle comporte un numéro de carte

bancaire, un code de vérification (CVV) et une date d'expiration. Cette carte n'étant générée que pour un achat unique, cela permet de limiter fortement les risques de piratage.

Si vous êtes intéressé par ce service, renseignez-vous auprès de votre banque pour en connaître les modalités.

## 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 deux 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 pas un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires, etc.) 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-y 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 **Commission nationale de l'informatique et des libertés (Cnil)** < <https://www.cnil.fr/> > : « 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 des caractères spéciaux, au moins une majuscule, un chiffre...).
- ▶ **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.

**En savoir plus sur les conseils à retenir pour assurer votre sécurité numérique**

## 7. En cas d'incident, contactez d'abord votre banque [≤ http://cybermalveillance.gouv.fr >](http://cybermalveillance.gouv.fr)

- ▶ 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 le **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.

### Ces contenus peuvent aussi vous intéresser

Comment acheter en ligne en toute sécurité

En savoir plus sur les conseils à retenir pour assurer votre sécurité numérique

Sécurité sur le web : découvrez le site web [cybermalveillance.gouv.fr](http://cybermalveillance.gouv.fr)

Dix règles pour vous prémunir contre le piratage de vos données personnelles

Comment créer un mot de passe sécurisé et simple à retenir ?

Que faire en cas de perte ou de vol de sa carte bancaire ?

### En savoir plus sur la sécurisation des paiements en ligne

Achats en ligne – 10 réflexes de sécurité <

<https://www.lesclesdelabanque.com/particulier/achats-en-ligne-10-reflexes-securite/>> le guide pratique, sur le site [lesclesdelabanque.com](http://lesclesdelabanque.com)

Ces 5 réflexes qui sécurisent votre paiement en ligne <

<https://www.cnil.fr/fr/ces-5-reflexes-qui-securisent-votre-paiement-en-ligne>> sur le site [Cnil.fr](http://Cnil.fr)

## Thématiques : [Achats sur internet](#)

---

Ce sujet vous intéresse ? Chaque mardi avec la lettre Bercy infos Particuliers, ne manquez aucune info pratique sur vos droits et obligations en matière de fiscalité, épargne, consommation ...

---

Partager la page   