



Les achats en ligne



Nous effectuons de plus en plus d'achats en ligne notamment par carte bancaire. Les sites marchands, fréquemment confrontés à la fraude, cherchent à s'en prémunir en demandant des justificatifs aux internautes. Comment acheter en ligne en toute sécurité ? Jusqu'où aller dans la communication de justificatifs ?

Quelles informations nécessaires pour acheter en ligne ?

Pour permettre l'achat de biens en ligne, un commerçant peut demander à ses clients un certain nombre d'informations permettant à la fois d'assurer la sécurité de la transaction et d'enrichir sa connaissance de ses clients. Si certaines informations sont obligatoires à la création d'un compte client (comme les coordonnées pour les livraisons), d'autres sont facultatives (c'est souvent le cas de la date de naissance). La réception de publicités est également facultative : aucun achat ne peut être conditionné à l'acceptation de recevoir une newsletter ou des sollicitations commerciales.

Les précautions à prendre lors d'un achat en ligne

Les pages sur lesquelles un client effectue une transaction (coordonnées, paiement en ligne) doivent utiliser une connexion sécurisée. Cela se traduit par une adresse qui commence par « <https://> » et par la présence d'une icône représentant un cadenas verrouillé dans la fenêtre du navigateur.

Conseil

Les plaintes reçues par la CNIL montrent qu'il est important de ne pas laisser un mineur effectuer seul un achat en ligne.

Numéro de carte bancaire : les utilisations à exclure

Le numéro de carte bancaire ainsi que le cryptogramme visuel doivent être saisis par le client internaute pour réaliser la transaction. Cependant, le site marchand doit faire une utilisation très limitée de ces informations.

Une fois le paiement effectué, le commerçant ne peut ni conserver ni réutiliser les coordonnées bancaires de son



client sans son consentement. Une conservation en base « archive » est néanmoins permise pendant 15 mois, délai de contestation du titulaire de la carte. Le cryptogramme visuel ne doit pas être conservé.

La CNIL veille !

La CNIL a adressé avertissement public à une société d'e-commerce qui avait conservé les numéros des cartes bancaires de ses clients sans leur consentement.

Comment se protéger lors d'un achat en ligne ?

Les usurpations d'identité et les utilisations frauduleuses de cartes bancaires sont plus fréquentes dans le commerce en ligne (il n'est en effet pas nécessaire de saisir le code de sa carte comme dans un commerce physique). Le commerçant doit donc se prémunir contre ces fraudes, autant dans son intérêt que dans celui de ses clients. En effet, en cas de contestation par le titulaire de la carte dans un délai de 15 mois après la transaction, le commerçant se verra retirer par sa banque le montant qu'il avait perçu.



• 3D Secure

Le commerçant peut utiliser un système appelé « 3D Secure » de Visa et Mastercard : lorsque l'internaute renseigne les informations de sa carte bancaire, il doit également fournir un code à usage unique qui lui est adressé par sa banque par sms sur son téléphone mobile (la banque ayant auparavant demandé ce numéro à son client pour cette action).

À défaut de renseigner ce code, la transaction ne pourra pas s'effectuer.

• La garantie de paiement

Le commerçant peut sinon faire appel à un prestataire de service qui lui garantira ou non le paiement des transactions. À partir d'éléments statistiques (par exemple, le montant moyen du panier sur le site) et sur la base des éléments figurant sur le bon de commande de l'internaute (date et heure, montant, type de produit, adresse, etc.), le prestataire va définir un niveau de risque acceptable ou non par le commerçant. Si la transaction est considérée comme non risquée le paiement et la livraison s'effectueront normalement et en cas de contestation ultérieure le prestataire remboursera le commerçant.

En revanche, si la transaction est considérée à risque par le prestataire, le commerçant peut demander des justificatifs à l'internaute. À défaut de présenter ces justificatifs, le commerçant peut annuler la commande. **Ces justificatifs peuvent être demandés avant ou après le paiement en ligne.**

Quelles garanties ?

Le commerçant, pour s'assurer de l'identité du détenteur de la carte bancaire, peut demander un justificatif d'identité et / ou de domicile. En revanche, il ne peut pas demander un relevé de compte ou une photocopie de la carte vitale ou du RIB. Seuls les services du commerçant en charge du paiement ou de la lutte contre la fraude doivent avoir accès à ces documents. Ils ne peuvent les utiliser à d'autres fins ni les conserver au-delà de six mois.

Pour éviter que des personnes non autorisées accèdent à ces informations, le site doit prendre toutes les mesures de sécurité utiles (page sécurisée du compte client pour l'envoi des pièces jointes).

Ne jamais envoyer une photocopie de sa carte bancaire !
L'envoi du seul recto de la pièce d'identité suffit à contrôler l'identité.
Les photocopies en noir et blanc permettent d'éviter les utilisations frauduleuses.

L'information des consommateurs

La conservation des données figurant sur la carte bancaire, afin de faciliter les achats futurs, est soumise au recueil du consentement de son titulaire. Une case à cocher, non pré-cochée, est un bon moyen de recueillir ce consentement. L'acceptation des conditions générales d'utilisation du site ne suffit pas.

Si un dispositif de contrôle (demande de pièces justificatives) est mis en place, il doit être mentionné dans les conditions générales d'utilisation du site ainsi que lors de chaque acte d'achat. Les internautes doivent également être informés de leurs droits :

Exemple de formulation

Afin d'optimiser la sécurité des paiements, nous procédons à des demandes de justificatifs complémentaires dont les seuls destinataires sont XXX. En cas de défaut de réponse, nous nous réservons la possibilité d'annuler la commande.
Vous disposez d'un droit d'accès et de rectification auprès de XXX.

Quelles formalités CNIL ?

Un fichier de clients d'un site d'e-commerce peut faire l'objet d'une déclaration de conformité à la norme n°48 (déclaration simplifiée). Les dispositifs qui n'entrent pas dans le cadre de cette norme doivent faire l'objet d'une déclaration normale ou dans certains cas, d'une demande d'autorisation (lutte contre la fraude).

Si la société qui a créé le fichier a désigné un Correspondant Informatique et Libertés (CIL), celui-ci doit seulement noter le dispositif dans son registre.

Quels recours ?

- le service des plaintes de la CNIL, (la CNIL n'est pas compétente en cas de défaut de livraison),
- le procureur de la République,
- la direction départementale de la concurrence, de la consommation et de la répression des fraudes (DDCCRF).

Textes de référence

- **Le code monétaire et financier :**
[Article L133-24](#) (délai de contestation d'un paiement).
- **Le code pénal :**
[Articles 226-1](#) et suivants (protection de la vie privée).
[Articles 226-16](#) et suivants (atteintes aux droits des personnes résultant des traitements informatiques).
- [La loi du 6 janvier 1978](#)
- **Délibération de la CNIL :**
- [Norme simplifiée n° 48](#)

Voir aussi...

- Recours en cas de litige à la suite d'un achat à distance :
<http://vosdroits.service-public.fr/particuliers/F10868.xhtml>
- Le guide du vendeur d'e-commerce de la DGCCRF :
http://www.economie.gouv.fr/files/directions_services/dgccrf/documentation/publications/depliants/guide_ecommerce_mai2013.pdf

Contact CNIL

Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur www.cnil.fr. Vous pouvez également appeler la permanence juridique de la CNIL au 01 53 73 22 22, du lundi au vendredi de 10h à 12h et de 14h à 16h.