



ACHETER EN TOUTE SÉCURITÉ AVEC SA CARTE BANCAIRE

La protection des opérations par carte bancaire nécessite un degré élevé de sécurité, qu'il s'agisse de paiement ou retrait de proximité (ex : chez un commerçant) ou de paiement à distance. En tant que détenteur d'une carte LCL vous avez un rôle essentiel dans l'utilisation sécurisée de votre moyen de paiement. Vérifiez vos achats régulièrement en consultant vos comptes via Internet et votre relevé de compte dès réception. Assurez-vous que votre conseiller LCL a toujours vos coordonnées (téléphone, mail) à jour. En cas d'opération douteuse, LCL peut avoir besoin de vous joindre rapidement.

LE PAIEMENT SUR INTERNET

Lors de paiements sur internet, vous devez adopter des réflexes de prudence quant à la conservation et à la protection des données de votre carte bancaire :

- Vérifiez que le site est sécurisé (https devant l'adresse du site, cadenas fermé ou icône d'une clé dans le navigateur),
- Privilégiez les sites commerçants connus et réputés (vérifiez les coordonnées : nom, adresse, téléphone, service clients, ...),
- N'enregistrez jamais les informations de votre carte en tant qu'identifiant commercial sur un site marchand. Les données de votre carte ne peuvent servir que pour réaliser une transaction, réserver un bien ou un service, s'abonner pour un paiement récurrent ou créer un compte client sur le site pour faciliter les achats ultérieurs,
- Ne communiquez jamais votre code confidentiel que ce soit par téléphone, courriel ou sur un site internet qui vous le demanderait,
- Notez le montant exact et la date de la transaction pour vérifier le montant qui sera débité sur votre compte,
- Réagissez immédiatement auprès de votre conseiller LCL si un débit ne correspond pas à l'achat effectué.

LA SOLUTION 3D SECURE (CODE PAR SMS)

Aujourd'hui des mécanismes permettent d'authentifier le porteur de la carte lors d'un paiement sur internet, c'est-à-dire de s'assurer que l'utilisateur est bien le détenteur légitime de la carte.

LCL offre à ses clients plusieurs moyens d'authentification répondant à ce besoin de sécurité :

- **3D Secure** : au moment de l'achat, après avoir saisi les 16 chiffres de votre numéro de carte, la date de validité et les 3 chiffres du cryptogramme visuel qui figure au dos de la carte et uniquement si le commerçant utilise le système 3D Secure, vous serez automatiquement redirigé vers le site 3D Secure de LCL. Un code à usage unique à 6 chiffres vous sera communiqué par LCL par SMS sur le numéro de téléphone renseigné dans nos fichiers clients. Après avoir vérifié que ce code, associé au commerçant et au montant communiqué dans le SMS, correspond à votre achat, vous devrez reporter ce code sur le site 3D Secure de LCL. Si le code saisi est correct, c'est le commerçant qui vous confirmera le paiement de la transaction.
 - o Pas d'inscription préalable à 3D Secure : le service est ouvert à tous les porteurs de carte LCL,
 - o Veillez à mettre à jour vos coordonnées téléphoniques auprès de votre conseiller LCL.

L'ENVIRONNEMENT

La sécurité des paiements en ligne passe également par la sécurité de l'ordinateur, du portable et des connexions liées. Il est indispensable de :

- Suivre les conseils de sécurité de votre fournisseur d'accès internet,
- Télécharger régulièrement les mises à jour système,
- Installer sur son ordinateur, tablette ou smartphone un antivirus et un pare feu efficaces avec des mises à jour automatiques,
- Ne pas garder en mémoire de votre navigateur ou de votre application mobile vos codes d'accès même si cela vous est proposé,
- En cas d'utilisation d'un réseau wi-fi, s'assurer que la configuration est sécurisée,
- Eviter de réaliser des transactions depuis un ordinateur ou un réseau wi-fi public,
- Ne jamais répondre aux appels téléphoniques ou courriels vous demandant des données personnelles (numéro de carte, numéro de compte, identifiant, mot de passe, code ...), d'accès à votre box internet, à votre banque en ligne, ou à toute autre sollicitation,
- N'utiliser jamais le lien figurant dans un courriel pour vous connecter à votre site de banque en ligne,
- Ne pas ouvrir et ne pas cliquer sur des liens contenus dans des courriels dont on ne connaît pas l'expéditeur,
- Modifier régulièrement vos mots de passe en évitant les mots de passe trop faciles à trouver (date de naissance, prénom des enfants,...),
- Réserver un mot de passe spécifique pour vos accès banque en ligne et d'une manière générale, ne pas utiliser le même mot de passe pour vos applications et sites internet.

Vous trouverez des conseils sur le site LCL Sécurité (<https://informations.lcl.fr/securite/>).

FAQ

- **Vous constatez une anomalie sur votre relevé de compte ou votre site de banque en ligne ?**
Contactez immédiatement LCL :
 - o Par téléphone au **09.69.36.30.30** (Prix d'un appel local non surtaxé pour tout opérateur en France Métropolitaine) du lundi au vendredi de 8h à 22h et le samedi de 8h à 17h30,
 - o 24h/24 via la messagerie sécurisée de votre banque en ligne,
 - o Si vous n'êtes pas à l'origine de l'opération, vous disposez de 13 mois pour la contester si elle a été effectuée dans un pays de l'Espace Economique Européen ou de 90 jours pour les autres pays,
 - o S'il s'agit d'une opération que vous avez autorisée mais dont vous ne connaissiez pas le montant exact (abonnement par exemple) et que celui-ci excède ce à quoi vous pouviez raisonnablement vous attendre, vous disposez de 8 semaines pour le contester.
- **Vous recevez un SMS « Alerte LCL » indiquant une transaction internet enregistrée par votre carte ?**
 - o Rappelez immédiatement 24h/24 le numéro indiqué sur le SMS soit pour confirmer que vous êtes bien à l'origine de la transaction et lever le doute, soit confirmer qu'il s'agit d'une fraude. Toutes les informations nécessaires pour la suite à donner vous seront communiquées par nos opérateurs dédiés.
- **Vous n'avez pas reçu le code à usage unique destiné à vous authentifier pour un paiement sur un site 3D Secure ?**
 - o La transaction qui n'a pas pu être sécurisée est abandonnée. Il s'agit vraisemblablement d'un problème sur le réseau de l'opérateur téléphonique. Renouvelez l'opération ultérieurement.

Ces informations sont données à titre indicatif et peuvent donner lieu à des modifications selon l'évolution de la réglementation.

10/2016

- **Vous vous apercevez que votre téléphone (fixe ou mobile) ne fonctionne plus ?**
 - o Contactez immédiatement votre opérateur téléphonique pour vous assurer que vous n'êtes pas victime d'un détournement de ligne. Des fraudeurs ayant eu accès à vos identifiants personnels de votre box ou de votre compte chez l'opérateur peuvent aisément détourner la ligne fixe vers un numéro anonyme ou se faire délivrer une nouvelle carte SIM leur permettant de récupérer les codes à usage unique transmis par votre banque,
 - o Vérifiez vos transactions d'achats et vos transactions bancaires en vous connectant sur votre site bancaire. Si vous constatez des opérations frauduleuses, contactez immédiatement votre conseiller.
- **Vous ne parvenez pas à faire de paiement sur internet ?**
 - o LCL dispose d'outils de surveillance et de détection de la fraude pour éviter au titulaire de la carte les désagréments liés aux utilisations frauduleuses de sa carte. Certains paiements sur internet peuvent ainsi être refusés pour des raisons sécuritaires ou réglementaires..

Enfin, si vous ne souhaitez pas faire d'achats à distance, sur internet ou par téléphone, LCL vous offre la possibilité de désactiver cette fonctionnalité de votre carte. N'hésitez pas à contacter votre conseiller.

Pour plus d'informations sur les risques Internet, les solutions, comment sécuriser son ordinateur, et même vous essayer à notre quizz sécurité, n'hésitez pas à consulter l'espace sécurité LCL, régulièrement mis à jour sur <https://informations.lcl.fr/securite/>.