DÉCEMBRE 2021

ACHATS EN LIGNE

10 RÉFLEXES SÉCURITÉ

www.lesclesdelabanque.com
Le site pédagogique sur la banque et l'argent

FÉDÉRATION BANCAIRE FRANÇAISE

N°2
LES GUIDES
SÉCURITÉ BANCAIRE

les clés de la banque

CE GUIDE VOUS EST OFFERT PAR

Pour toute information complémentaire,
nous contacter : info@lesclesdelabanque.com

Éditeur : FBF - 18 rue La Fayette 75009 Paris - Association Loi 1901
Directeur de publication : Maya Atig
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : décembre 2021

SOMMAIRE

ATTENTION

Fournir ses coordonnées bancaires peut exposer à des risques d'utilisation frauduleuse.
Voici quelques réflexes de sécurité à adopter.

1

Je vérifie que le site marchand est sûr

Même si vous utilisez régulièrement un site marchand, **vérifiez toujours que l'adresse du site est correcte** surtout si vous trouvez que sa page d'accueil ou ses modalités de fonctionnement vous semblent un peu différentes du site que vous utilisez habituellement. Tapez toujours vous-même l'adresse du site.

S'il s'agit de votre 1er achat sur le site, **vérifiez qu'il fournit :**

- des informations claires et complètes sur l'entreprise (nom, adresse, service clients),
- un contact (téléphone ou courrier électronique),
- des garanties de livraison et de retour,
- un accès à vos données personnelles et la possibilité de les corriger/supprimer,
- des conditions générales de vente et des modalités de paiement précises (carte débitée à la commande ou à l'expédition, ou encore après réception et vérification du bien acheté, etc.).

Passez par un site marchand connu et réputé. Consultez les avis des internautes à propos de ce site.

2

Je reste vigilant face à un courrier électronique

- **N'utilisez jamais le lien**, depuis par exemple un courrier électronique, ou une publication sur les réseaux sociaux, **pour vous connecter à un site commerçant et y réaliser un paiement** : tapez soigneusement l'adresse du site Internet (sans coquille ni faute).
- **Ne répondez jamais à un courrier électronique qui vous semble douteux** et qui utilise les coordonnées ou l'identité (logo, visuel…) d'un site commerçant. Ne fournissez jamais d'informations à l'expéditeur d'un tel message.
- Faites aussi **attention aux messages, SMS ou appels vocaux vous incitant à appeler ou rappeler un numéro** ou à vous connecter sur un site Internet en cliquant sur un lien.

Le phishing est un courrier électronique qui vous invite à vous connecter à un site de banque, un compte de paiement en ligne ou encore un site marchand. On vous demande par exemple de mettre à jour vos informations personnelles ou de régulariser une facture impayée… Le lien conduit en réalité vers le site Internet d'un escroc qui tente de récupérer vos coordonnées pour les utiliser à des fins frauduleuses.

3

Je protège les données de ma carte bancaire

Ne donnez jamais le code confidentiel de votre carte bancaire, à qui que ce soit.

Evitez de donner les informations de votre carte par courrier (électronique ou papier), par sms ou téléphone surtout si vous pouvez faire autrement (paiement par Internet...). Ne donnez les informations et données de votre carte qu'à un commerçant dont vous êtes sûr.

Pour un achat en ligne, ou pour réserver un bien ou service, **on peut vous demander** :

- **le n° de votre carte bancaire** : 16 chiffres (au recto),
- **la date d'expiration** (au recto),
- **le cryptogramme** : 3 derniers chiffres imprimés (au verso, le cryptogramme peut être dynamique, il change régulièrement),
- **le nom et éventuellement le prénom** (au recto).

Depuis mai 2021, une authentification forte est exigée pour payer un achat en ligne par carte. Il peut s'agir par exemple de se connecter à l'appplication de votre banque avec votre smartphone pour valider l'opération ou de fournir un code que vous seul connaissez.
Des exemptions sont possibles notamment en cas de montant faible. L'objectif est de vérifier que la personne en train d'effectuer le paiement est le propriétaire de la carte.

Il est déconseillé d'enregistrer son numéro de carte bancaire dans les comptes clients des sites marchands qui le proposeraient.

4

Je choisis une solution adaptée pour mes achats en ligne

Il existe différentes solutions de paiement pour vos achats en ligne. Choisissez celle qui correspond le plus à vos besoins.

Des portefeuilles électroniques (aussi appelés « **wallets** ») sont proposés par exemple par certaines banques mais aussi par des groupes de commerçants, etc. Ce moyen de paiement digital permet de limiter la circulation des données carte. Chaque portefeuille électronique propose sa propre méthode d'authentification sécurisée.

!

ATTENTION

Même simplifié, cela n'en reste pas moins un paiement et vous ne devez pas le banaliser. Soyez prudent, comme vous l'êtes avec le code secret de votre carte bancaire : ne divulguez à personne vos codes d'accès à votre portefeuille électronique.

5

Je contacte ma banque en cas de doute

Vous pensez avoir communiqué à un faux commerçant les données de votre carte ?

- **Si vous avez fourni vos informations personnelles et numéros de carte, contactez immédiatement le service clients de votre banque** ou votre conseiller bancaire pour leur signaler et faire opposition sur votre carte. Surveillez votre compte et en cas de débit frauduleux, contestez l'opération auprès de votre banque.
- Si vous n'avez pas fourni vos informations personnelles et numéros de carte, ne vous inquiétez pas ; sans ces informations les escrocs ne peuvent rien faire.

Vous pouvez signaler la tentative de fraude au commerçant dont l'identité a été utilisée.

6

Je consulte régulièrement mon compte

Seule une consultation régulière de votre compte peut vous permettre de détecter un incident.

Connectez-vous souvent et au moins chaque semaine sur le site de votre banque à distance/votre application mobile, ou vérifiez le contenu de votre relevé de compte dès sa réception avec les factures, le courrier électronique de confirmation de paiement ou encore sur l'espace client du site commerçant.

Lors d'un achat, notez le nom du commerçant, le montant exact et la date de l'opération qui passera sur votre compte, vérifiez le montant qui vous sera débité pour réagir immédiatement auprès de votre banque en cas d'anomalie.

7

Je signale rapidement toute anomalie

En cas de doute sur une opération, prévenez immédiatement votre banque par téléphone et par courrier électronique. Selon la nature de l'opération anormale relevée, votre banque pourra faire des recherches.

S'il s'agit vraiment d'une opération que vous n'avez pas faite (« opération non-autorisée » ou « mal exécutée »), **signalez rapidement l'anomalie à votre banque et au plus tard dans les :**

- **13 mois suivant la date du débit pour un paiement dans l'Espace Economique Européen - EEE*,**
- **70 jours suivant la date du débit, pour un paiement hors de l'EEE.** Ce délai peut être prolongé contractuellement à 120 jours.

**Les pays de l'EEE sont les 27 pays de l'Union européenne et l'Islande, le Liechtenstein, la Norvège.*

En cas de doute sur une opération, demandez sans attendre des précisions à votre banque. Si les données de votre carte ont été subtilisées, vous devez faire opposition pour bloquer la carte et la rendre inutilisable.

Sauf si des investigations s'avèrent nécessaires, le remboursement des opérations non-autorisées s'effectue, au plus tard, le lendemain de la contestation (en jour ouvrable).

8

Pour tout litige commercial, je m'adresse au commerçant

Vous n'avez pas été livré ? Le bien livré n'est pas conforme au bien attendu ? Vous avez accepté de recevoir un échantillon mais des débits « carte » passent ensuite tous les mois pour recevoir des produits que vous n'avez jamais commandés, etc. ?

Il s'agit de **litiges commerciaux. La banque ne peut pas intervenir** dans ces litiges : c'est avec le commerçant que vous devez dialoguer.

Si le commerçant et vous-même résidez au sein de l'Union européenne, vous pouvez utiliser la **plateforme européenne de résolution de litiges en ligne** afin d'obtenir un règlement extrajudiciaire.

9

Je protège mon matériel

La sécurité de vos paiements passe par la sécurisation de vos terminaux (ordinateur, mobile, etc.).

- Téléchargez régulièrement les mises à jour de votre système, installez sur votre ordinateur, comme sur votre mobile, un antivirus et un pare-feu efficaces avec des mises à jour automatiques.
- N'ouvrez pas un message douteux avec un objet et un contenu passe-partout, surtout si une pièce jointe est attachée, détruisez-le sans l'ouvrir.
- N'effectuez aucun paiement si vous pensez avoir un virus sur votre ordinateur.
- N'utilisez pas un équipement (ordinateur ou mobile) dont vous ne maîtrisez pas le niveau de sécurité.
- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes, jeux…) provenant d'une source fiable.
- Verrouillez votre smartphone, tablette par un schéma de sécurité ou un code (en plus du mot de passe pour déverrouiller la carte SIM) ; en cas de vol, cela rendra plus difficile son utilisation et la consultation de son contenu.

10

Je sécurise mes connexions

- **Choisissez un fournisseur d'accès Internet reconnu et suivez ses conseils de sécurité.**
- Evitez les sites compromis à l'aide d'un logiciel de sécurité bloquant l'accès aux sites de commerçants falsifiés.
- Vérifiez que le site Internet est sécurisé (**« https » devant l'adresse du site, ou cadenas fermé**, ou icône d'une clé dans le navigateur).
- Choisissez avec soin vos mots de passe : de préférence alphanumérique et différent de celui de votre service de banque à distance.
- N'activez la fonction Bluetooth ou Wi-Fi que lorsque c'est nécessaire et désactivez-la dès la fin d'utilisation.

- **Evitez les achats depuis un ordinateur public ou connecté à un réseau Wi-Fi public.** Si vous utilisez un réseau Wi-Fi, assurez-vous que la configuration est sécurisée.
- **Déconnectez-vous** du site après avoir effectué votre achat.

Le Bluetooth est une technologie de réseau sans fil de faible portée permettant de relier des appareils entre eux (par exemple imprimante, téléphone portable, souris, clavier, etc.).

Le Wi-Fi (« Wireless Fidelity ») est une norme de réseau sans fil utilisant des ondes radios entre l'ordinateur ou téléphone portable et un routeur Wi-Fi connecté à une prise téléphonique, chez vous ou à l'extérieur (par exemple : dans certains lieux publics, les hôtels...).

LES RÉFLEXES SECURITÉ POUR MES ACHATS EN LIGNE

1. Je vérifie que le site marchand est sûr
2. Je reste vigilant face à un courrier électronique
3. Je protège les données de ma carte bancaire
4. Je choisis une solution adaptée pour mes achats en ligne
5. Je contacte ma banque en cas de doute
6. Je consulte régulièrement mon compte
7. Je signale rapidement toute anomalie
8. Pour tout litige commercial, je m'adresse au commerçant
9. Je protège mon matériel
10. Je sécurise mes connexions

les clés de la banque