FÉVRIER 2015

# ACHATS EN LIGNE

## 10 RÉFLEXES SÉCURITÉ

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

**www.aveclespme.fr**
Le site pratique pour les PME

FEDERATION BANCAIRE FRANCAISE

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 : Marie-Anne Barbat-Layani
Imprimeur : Concept graphique,
ZI Delaunay Belleville - 9 rue de la Poterie - 93207 Saint-Denis
Dépôt légal : février 2015

# SOMMAIRE

# ATTENTION

**Donner ses coordonnées de compte bancaire sans vérification vous expose à des risques.**

Soyez vigilant !

1

# Je vérifie que le site du commerçant est sûr

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

S'il s'agit de votre premier achat sur ce site, **vérifiez les points suivants** :

- Les informations sur l'entreprise doivent être claires et complètes (nom, adresse, service clients).
- On doit pouvoir les contacter par téléphone ou courrier électronique.
- Les garanties de livraison et de retour doivent être indiquées.
- Vous devez pouvoir accéder à vos données personnelles et demander leur correction ou suppression.
- Les Conditions Générales de Vente du site marchand doivent décrire précisément les modalités applicables sur le site : carte débitée à la commande ou à l'expédition ou encore après réception et vérification du bien acheté, etc.

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

2

# Je reste vigilant face à un courrier électronique

- **N'utilisez jamais le lien** figurant dans un courrier électronique **pour vous connecter à un site commerçant et y réaliser un paiement** : c'est à vous de saisir l'adresse du site internet du commerçant.
- **Ne répondez jamais à un courrier électronique douteux** utilisant 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 ou SMS vous incitant à appeler un numéro** ou à vous connecter.

*Attention : contraction des mots anglais « fishing », (pêche) et « phreaking » (piratage de lignes téléphoniques), le phishing est un courrier électronique qui vous invite, souvent sous prétexte de sécurité, à vous connecter à un site de banque, un compte de paiement en ligne ou encore un site commercial (ou à appeler un numéro de téléphone ou envoyer un SMS). Le lien ou le numéro conduit en fait vers un pirate. L'accroche peut aussi se faire par téléphone ou SMS, on parle alors de « vishing » et de « smishing ».*

3

# Je protège les données de ma carte bancaire

- **Ne donnez jamais le code confidentiel de votre carte bancaire, à qui que ce soit.**
- **N'enregistrez jamais les informations de votre carte** (numéro, date, cryptogramme) **en tant qu'identifiant commercial** sur un site marchand.
- **Evitez de donner les informations de votre carte** par courrier (électronique ou papier), par sms ou téléphone 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 une réservation, on peut vous demander :*

- *le numéro de votre carte bancaire : 16 chiffres (au recto),*
- *la date d'expiration (au recto),*
- *le cryptogramme : 3 derniers chiffres imprimés (au verso à côté de la zone de signature),*
- *le nom et éventuellement le prénom (au recto)*
- *un code supplémentaire de type 3DSecure sur certains sites marchands *. Envoyé par sms, courrier électronique, téléphone (le SMS étant le plus souvent utilisé), ce code permet de vérifier que la personne en train d'effectuer le paiement est bien le propriétaire de la carte.*

**Tous les paiements par carte sur internet ne sont pas concernés par ce système ; certains sites commerçants, y compris de grands acteurs, n'ont pas ce dispositif de protection pour le client.*

4

# Je choisis une solution adaptée pour mes achats en ligne

**Vérifiez avec la banque les solutions qu'elle propose pour vos achats en ligne.**

**EXEMPLE**

*Des portefeuilles électroniques* ***(aussi appelés «*** *wallets* ***») sont proposés par certaines banques mais aussi des groupes de commerçants, des opérateurs de téléphonie, etc. Il s'agit de confier à un « tiers de confiance » vos données personnelles et de paiement, qui sont stockées en vue de réaliser des opérations de paiement. Vous regroupez ainsi plusieurs cartes (de paiement, de fidélité, etc.).*

*Vous n'avez plus à saisir ni le cryptogramme visuel ni le code 3D Secure qu'on demande habituellement lors d'un usage classique de la carte bancaire. Les données carte ne sont pas communiquées au site marchand.*

**ATTENTION**

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

5

# Je contacte ma banque en cas de doute

Vous pensez avoir communiqué à un faux commerçant les données de votre carte sur internet (phishing) ou par téléphone (vishing) ?

- **Si vous avez fourni vos informations personnelles et numéros de carte, contactez immédiatement le service relations clients** 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 pirates ne peuvent rien faire.

*Signalez la tentative de fraude au commerçant concerné.*

6

# Je consulte régulièrement mon compte

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

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

*Lors d'un achat, notez 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 ou courrier électronique et confirmez par lettre. Selon la nature de l'opération, votre banque pourra faire des recherches.

S'il s'agit vraiment d'une opération que vous n'avez pas faite (dite « 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.

**Au 1er janvier 2014, les pays de l'EEE sont les 28 pays de l'Union Européenne et l'Islande, le Liechtenstein, la Norvège.*

**ATTENTION**

**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.**

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 voulus, 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.

!

**ATTENTION**

**... aux abonnements, échantillons et autres offres « incroyables » : Lisez bien les conditions générales de vente avant de les accepter.**

9

# Je protège mon matériel

**La sécurité de vos paiements passe par la sécurisation de vos terminaux** (ordinateur, téléphone portable, tablettes 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 smartphone) dont vous ne maîtrisez pas le niveau de sécurité.
- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes pour mobile et jeux) provenant d'une source fiable.
- Verrouillez votre mobile (smartphone, tablette) par un schéma de sécurité ou un code (en plus du mot de passe pour 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 (chiffres + lettres) et différent de celui de votre service 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.

*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...).*



# ACHATS EN LIGNE
# 10 RÉFLEXES SÉCURITÉ

1. **Je vérifie que le site du commerçant 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