Banque à distance

10 RÉFLEXES SÉCURITÉ

les clés de la banque

LES GUIDES BANCAIRES
N°4 / Sécurité

CE GUIDE VOUS EST OFFERT PAR :

les clés de la banque

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 : mars 2025

SOMMAIRE

10 RÉFLEXES SÉCURITÉ

Introduction

En tant que client de la banque, votre rôle est essentiel dans l'utilisation sécurisée des services de banque à distance. Comme avec vos papiers d'identité ou vos clés, vous devez faire attention à vos données bancaires personnelles. En les protégeant, vous vous protégez.

1. Je consulte les consignes de sécurité de ma banque

Les banques proposent sur leur site Internet et leur application mobile une **rubrique consacrée à la sécurité**. Elle contient les **dispositifs en vigueur**, des **alertes** et mises en garde **contre les fraudes du moment**... Elle rappelle les principes de précaution pour vos données bancaires, et notamment vos données de sécurité personnalisées. **Consultez-la régulièrement et appliquez les consignes.**

L'accès à distance à vos comptes exige une authentification forte (générateur de code unique, lecteur de carte à puce, application mobile de la banque...), demandée au moins tous les 180 jours. Votre conseiller bancaire peut répondre à vos questions sur ce sujet.

2. **Je choisis avec soin mon mot de passe**

Votre mot de passe est personnel et confidentiel.
Il vous permet d'être le seul à pouvoir accéder à votre service de banque à distance.

- Changez le mot de passe provisoire dès réception.
- **Utilisez un mot de passe unique** pour la banque à distance : ne l'utilisez pas pour d'autres applications ou sites Internet.
- **Évitez les mots de passe trop faciles** à trouver (date de naissance ou série du genre « 123456 » ou « 000000 »…).
- **Modifiez-le régulièrement.**

Sur certaines applications bancaires, et en fonction du téléphone, il est possible de s'authentifier par des procédés biométriques (empreinte digitale, reconnaissance faciale…).

3. Je garde mes codes d'accès et de validation secrets

Votre banque ne vous demandera jamais vos mots de passe ou vos codes.

- **Ne divulguez à personne vos identifiants et mots de passe** (ni à votre banque, ni à la police, ni à votre famille, etc.) car ils sont strictement personnels et confidentiels. Ainsi, personne n'a à les connaître.
- Conservez-les hors de portée de quiconque. **Ne les enregistrez pas** sur votre mobile, tablette, ordinateur, ni dans un fichier ou un espace non sécurisé. Ne les notez pas non plus sur un papier « scotché » à votre carte bancaire (ou placé à proximité).
- Si vous utilisez l'appareil de quelqu'un, veillez à ce que la fonction d'enregistrement de l'identifiant ou du mot de passe soit désactivée.
- Assurez-vous que personne ne voie vos codes lorsque vous les saisissez et **changez-les** si vous pensez qu'ils ont été compromis.

Communiquer à quelqu'un votre identifiant et votre mot de passe de banque à distance, ce serait lui permettre d'avoir accès à vos comptes bancaires et ainsi lui permettre d'effectuer éventuellement des opérations frauduleuses.

Vous êtes le seul à pouvoir valider une opération en ligne (virement, ajout de bénéficiaire, etc.). Cette validation doit toujours être à votre initiative et ne jamais faire suite à la demande d'un tiers. Ne communiquez jamais vos codes de validation ni aucune information sensible à qui que ce soit.

4. **Je ne me connecte jamais via un mail, SMS, QR code**

La connexion à votre banque à distance doit toujours être à votre initiative et jamais sollicitée par quelqu'un.

Pour éviter le phishing, SMShing ou Vishing (récupération et détournement de vos codes et d'autres données personnelles ou bancaires, par mail, SMS ou appel) :

- **Ne suivez jamais un lien** provenant d'un e-mail, QR code, SMS pour accéder à votre banque à distance, quel qu'en soit l'objet. **Saisissez toujours l'adresse du site vous-même** dans votre navigateur.
- Signalez le SMS au 33700, numéro mis en place par les principaux opérateurs français pour lutter contre ces fraudes : plus d'informations sur www.33700.fr.
- **Ne donnez pas suite à un courrier électronique douteux** et utilisant les coordonnées ou l'identité (logo, visuel…) de votre banque, surtout si l'objet est alarmiste et demande une action urgente.
- **Ne fournissez aucune information** à l'expéditeur d'un tel message. Prévenez votre banque au plus vite, aux coordonnées habituelles, en lui faisant suivre le message.

ATTENTION Votre banque ne vous demandera jamais de vous connecter via un lien présent dans un SMS ou un mail.

5. **Je contacte ma banque en cas de doute**

Si vous pensez avoir fourni vos codes d'accès de banque à distance à un tiers, **alertez immédiatement votre banque, aux coordonnées habituelles** et non celles présentes dans les messages reçus. En effet, vous risquez que les fraudeurs accèdent à vos données bancaires et essaient d'effectuer des opérations à votre insu.

Sans attendre les instructions de la banque :

- **lancez l'antivirus et changez vos codes d'accès** ;
- **vérifiez les dernières opérations effectuées**, celles en attente ainsi que les bénéficiaires de virement enregistrés ;
- **signalez la tentative d'escroquerie** sur www.internet-signalement.gouv.fr (Pharos) et www.signal-spam.fr.

6. **Je consulte régulièrement mon compte**

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

Connectez-vous régulièrement (au moins **une fois par semaine**) sur le site de votre banque à distance ou l'application mobile.

Vérifiez/comparez **les débits sur votre relevé de compte** notamment avec les talons des chèques émis, les tickets de carte et les courriels de confirmation de paiement (reçus par exemple pour les achats par Internet).

Assurez-vous que vos coordonnées sont à jour auprès de votre banque (téléphone, email). En cas d'opération douteuse, elle peut avoir besoin de vous joindre rapidement.

7. Je signale rapidement toute anomalie

Si vous identifiez une opération que vous n'avez pas effectuée, prévenez immédiatement votre banque.

Selon la nature de l'opération anormale relevée, votre banque pourra faire des recherches et vous indiquera la marche à suivre.

ATTENTION En cas de doute sur une opération, demandez sans attendre des précisions à votre banque.

8. Je réagis en cas d'activité suspecte sur mon téléphone

Le téléphone sert souvent à accéder à sa banque à distance (par Internet ou par une application) et à recevoir des codes de confirmation pour des opérations « sensibles » (virement par exemple) ou des achats en ligne. Vous devez donc être vigilant.

Réagissez rapidement et **contactez votre banque**, voire votre opérateur téléphonique si :

- **Vous recevez un SMS de sécurité alors que vous n'êtes pas en train de faire une opération « sensible » ou un achat en ligne.** Il s'agit sans doute d'une tentative de fraude ou d'une erreur de coordonnées ;
- **Votre ligne téléphonique rencontre des dysfonctionnements.** Suite à une usurpation d'identité, votre ligne pourrait avoir été détournée et être utilisée pour effectuer des tentatives de fraudes sur vos comptes.

Si vous pensez être victime d'une escroquerie, contactez info-escroqueries au 0 805 805 817 (service et appel gratuits).

9. Je protège mon matériel

La sécurité de vos appareils (ordinateur, téléphone, tablette) est primordiale pour contrer les virus et logiciels malveillants.

- **Téléchargez régulièrement les mises à jour système**, installez un antivirus et un pare-feu efficaces avec des mises à jour automatiques.
- **N'ouvrez pas un message suspect**, encore moins la pièce jointe. Supprimez-le sans l'ouvrir.
- **N'effectuez aucune opération bancaire** (connexion, virement, opposition…) **si vous pensez avoir un virus.** Lancez l'antivirus pour nettoyer l'appareil. En cas de virus avéré, contactez votre banque pour obtenir de nouveaux codes d'accès.
- N'utilisez pas un équipement dont vous ne maîtrisez pas le niveau de sécurité (cybercafé, etc.).
- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes, jeux…) provenant d'une source fiable.

En cas de perte ou de vol de votre appareil, changez au plus vite vos mots de passe (banque, applications, email).

ATTENTION **Verrouillez votre smartphone, tablette avec un code de sécurité (c'est mieux qu'un schéma) en plus du mot de passe de la carte SIM. Cela compliquera son utilisation et la consultation de son contenu en cas de perte ou vol.**

10. **Je sécurise mes connexions**

- Choisissez un fournisseur d'accès Internet connu et suivez ses conseils de sécurité.
- **Tapez vous-même l'adresse du site** et vérifiez les signes de sécurité (https, cadenas ou clé dans le navigateur). Cela garantit le cryptage des données échangées. Attention cependant, ça ne garantit pas que le site est officiel.
- Assurez-vous qu'aucune autre fenêtre Internet n'est ouverte.
- Activez le Bluetooth et le Wi-Fi seulement si c'est nécessaire et désactivez-le après utilisation.
- **N'accédez pas à votre banque à distance depuis un ordinateur public ou un réseau Wi-Fi public.**
- Vérifiez la date de votre dernière connexion si elle est affichée. Quand vous avez terminé, déconnectez-vous et effacez l'historique.
- **Videz la corbeille** si vous avez supprimé des documents.

LES RÉFLEXES CLÉS

Banque à distance

1. Je consulte les consignes de sécurité de ma banque
2. Je choisis avec soin mon mot de passe
3. Je garde mes codes d'accès et de validation secrets
4. Je ne me connecte jamais via un mail, SMS, QR code
5. Je contacte ma banque en cas de doute
6. Je consulte régulièrement mon compte
7. Je signale rapidement toute anomalie
8. Je réagis en cas d'activité suspecte sur mon téléphone
9. Je protège mon matériel
10. Je sécurise mes connexions

lesclesdelabanque.com

FÉDÉRATION
BANCAIRE
FRANÇAISE