JANVIER 2022

Ce guide a été élaboré
avec la Police Judiciaire

BANQUE À DISTANCE

10 RÉFLEXES SÉCURITÉ

N°4
LES GUIDES
SÉCURITÉ BANCAIRE

les clés de la banque

Ce guide a été élaboré avec la Direction Centrale de la Police Judiciaire.

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 : janvier 2022

SOMMAIRE

ATTENTION

En tant que client de la banque, vous avez un rôle essentiel à jouer 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 régulièrement les consignes de sécurité de ma banque

Pour informer leurs clients sur les dispositifs en vigueur, **les banques publient sur leur site Internet une rubrique consacrée à la sécurité**, notamment des alertes et mises en garde. **Consultez-la régulièrement et appliquez les consignes.**

Souvent détaillée, cette rubrique rappelle les principes de sécurité concernant vos données personnelles et bancaires, votre matériel et les risques sur Internet.

L'accès à distance à vos comptes nécessite une authentification forte (mobile, générateur de code unique, lecteur de carte à puce, application mobile de la banque…). Elle vous sera demandée tous les 90 jours, a minima, pour vous connecter à votre espace client. Votre conseiller bancaire pourra vous aider en cas d'interrogations sur ces modalités.

2

Je choisis avec soin mon mot de passe

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

- Changez votre mot de passe provisoire dès réception.
- **Réservez un mot de passe à la seule banque à distance**, ne l'utilisez pas pour d'autres applications ou sites Internet.
- **Evitez les mots de passe trop faciles** à trouver (date de naissance, mot du dictionnaire, prénoms familiaux…).
- **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 secrets mes codes d’accès

Même votre banque ne vous demandera jamais votre mot de passe.

D'une manière générale, **ne divulguez à personne votre identifiant et votre mot de passe** (ni à votre banque, ni à la police, ni à votre famille, etc.) car personne n'a besoin de les connaitre.

Conservez-les en sécurité et hors de portée de quiconque. Ne gardez pas vos codes d'accès en mémoire sur le terminal (mobile, tablette par exemple), ni dans un fichier ou sur un espace non sécurisés. Si vous utilisez l'équipement de quelqu'un, veillez à ce que la fonction d'enregistrement du mot de passe ne soit pas activée.

Assurez-vous que personne ne peut vous voir les saisir et changez-les si vous pensez que quelqu'un a pu les découvrir.

4

Je ne me connecte jamais à partir d'un courrier électronique ou SMS

Le phishing est une technique très répandue que vous devez savoir reconnaître.

IDENTIFIER LES TENTATIVES DE PHISHING

Le phishing est un courrier électronique qui vous demande de vous connecter (souvent pour mettre à jour vos informations personnelles ou pour bénéficier d'un remboursement, etc.) à un site de banque, un compte de paiement en ligne ou encore un site commercial, le site des impôts, de la CAF…

Le message est souvent alarmiste et insiste sur le caractère urgent de votre action. Le lien conduit en réalité vers un site pirate destiné à récupérer vos données personnelles et bancaires.

L'approche peut aussi se faire par téléphone ou SMS. On vous demande d'appeler ou rappeler un numéro de téléphone ou d'envoyer un SMS. On parle alors de « vishing » et de « smishing ».

RÉAGIR À UNE TENTATIVE DE PHISHING

- **Ne cliquez jamais sur un lien**, figurant par exemple dans un courrier électronique, pour vous connecter à votre site de banque à distance, quel qu'en soit l'objet : c'est à vous de saisir l'adresse du site Internet de votre banque.
- **Ne répondez jamais 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 jamais d'informations à l'expéditeur d'un tel message. Prévenez votre banque au plus vite en lui faisant suivre le message.

RÉAGIR À UNE TENTATIVE DE VISHING/SMISHING

Si vous recevez un appel téléphonique, **ne donnez aucune information de connexion à votre banque à distance**. Votre banquier ne vous demandera jamais votre mot de passe.

Si vous recevez un SMS vous demandant d'appeler un numéro, de vous connecter à un site depuis votre téléphone, **n'y répondez pas et n'appelez pas.**

Transmettez le SMS au 33700, numéro mis en place par les principaux opérateurs français pour lutter contre ces fraudes : plus d'informations sur **www.33700-spam-sms.fr**

Votre banque ne vous contactera jamais via un SMS ou un e-mail pour vous demander de vous connecter à son site ou à l'application bancaire.

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 via un site Internet, un lien SMS ou directement par téléphone, **contactez immédiatement votre banque**, aux coordonnées habituelles (n'utilisez pas celles des messages que vous venez de recevoir), pour lui signaler. Sinon, vous risquez que les pirates accèdent à vos données bancaires et effectuent des opérations à votre insu.

Sans attendre les instructions de la banque, lancez l'antivirus, changez vos codes d'accès, vérifiez les dernières opérations effectuées.

Pour signaler un site ou un courrier d'escroquerie, rendez-vous sur www.internet-signalement.gouv.fr 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.

Vérifiez/comparez les débits sur votre relevé de compte dès sa réception notamment avec les talons des chèques émis, les facturettes de carte et les courriels de confirmation de paiement (fournis la plupart du temps pour les achats par Internet).

Connectez-vous souvent et au moins une fois par semaine sur le site de votre banque à distance ou votre application mobile.

Assurez-vous que votre banque a toujours vos coordonnées à jour (téléphone, adresse de courrier électronique...). En cas d'opération douteuse, elle peut avoir besoin de vous joindre rapidement.

7

Je signale rapidement toute anomalie

Si une opération ne vous concerne pas, 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.

8

Je réagis en cas d'activité suspecte sur mon téléphone

Le téléphone portable peut être utilisé pour se connecter au service de banque à distance (par Internet ou par une application). Il permet parfois de recevoir par SMS un code de confirmation pour une opération « sensible » sur la banque à distance (virement par exemple) ou pour un achat 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 téléphoniques ;
- **en cas de dysfonctionnement de votre ligne téléphonique.** Suite à une usurpation d'identité, la ligne pourrait être détournée et être utilisée pour effectuer des tentatives de fraudes bancaires sur vos comptes.

Si vous pensez être victime d'une escroquerie, vous pouvez utilement prendre contact avec info-escroqueries au **0 805 805 817** Service & appel gratuits

9

Je protège mon matériel

La sécurisation de vos terminaux (ordinateur, téléphone portable, tablette, etc.) est primordiale.

Vous devez lutter contre les virus et logiciels malveillants (malwares) de tous types. Ces programmes nocifs s'introduisent sur vos appareils.

En cas de perte ou de vol d'un terminal (ordinateur, téléphone, tablette…), changez immédiatement vos mots de passe (applications bancaires et non bancaires), y compris vos codes d'accès de messagerie électronique.

- Téléchargez régulièrement les mises à jour système, installez sur vos appareils un antivirus et un pare-feu efficaces avec des mises à jour automatiques.
- N'ouvrez pas un message douteux (objet et contenu passe-partout), surtout si une pièce jointe est attachée, détruisez-le sans l'ouvrir.
- N'effectuez aucune opération de banque à distance (connexion, virement, opposition…) si vous pensez qu'un virus s'est installé, lancez l'antivirus puis contactez votre agence pour demander de nouveaux codes d'accès.
- N'utilisez pas un équipement dont vous ne maîtrisez pas le niveau de sécurité (cybercafé, libre-service…).
- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes, jeux…) provenant d'une source fiable.


ATTENTION
Verrouillez votre smartphone, tablette par un code de sécurité (mieux qu'un schéma) en plus du mot de passe de la carte SIM. 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.
- **Tapez vous-même l'adresse exacte du site Internet de la banque**, fourni par votre conseiller clientèle.
- Vérifiez la présence du **https** (« s » pour secure) **devant l'adresse du site**, l'icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet.
- Contrôlez qu'aucune autre fenêtre Internet n'est ouverte.
- N'activez la fonction Bluetooth ou Wi-Fi que lorsque c'est nécessaire et désactivez-la dès la fin d'utilisation.
- **N'accédez pas à votre banque à distance depuis un ordinateur public ou connecté à un réseau Wi-Fi public.**
- Si la date de votre dernière connexion est affichée, vérifiez-la. Quand vous avez terminé, utilisez le bouton « déconnexion ».
- Si vous avez supprimé des documents, n'oubliez pas de vider la corbeille.

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...).

BANQUE À DISTANCE
LES RÉFLEXES SÉCURITÉ

1. Je consulte régulièrement les consignes de sécurité de ma banque.
2. Je choisis avec soin un mot de passe dédié uniquement à ma banque en ligne.
3. Je garde secrets mes codes d'accès.
4. Je ne me connecte jamais à partir d'un lien reçu par courrier électronique ou SMS.
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.

les clés de la banque

www.lesclesdelabanque.com

Le site pédagogique sur la banque et l'argent

FÉDÉRATION
BANCAIRE
FRANÇAISE