MAI 2015

Ce guide a été élaboré
avec la Police Judiciaire

BANQUE À DISTANCE

10 RÉFLEXES SÉCURITÉ

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

FEDERATION
BANCAIRE
FRANCAISE

N°4
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 : mai 2015

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.

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. 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.

Des alertes et mises en garde sont mises en ligne régulièrement sur les sites internet des banques.

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 (messagerie, identification sur des sites internet non bancaires…).
- **Evitez les mots de passe trop faciles** à trouver (date de naissance, prénom de vos enfants…) et/ou déjà utilisés (accès téléphone, alarme…).
- **Modifiez-le régulièrement.**

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 (tablette par exemple), ni dans un fichier ou sur un espace communautaire 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.

ATTENTION

Communiquer à quelqu'un votre identifiant et votre mot de passe de banque à distance, ce serait lui permettre de faire toutes les opérations possibles sur votre compte bancaire, comme par exemple des virements. Il pourrait ainsi vider vos comptes.

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 la contraction des mots anglais « fishing », (pêche) et « phreaking » (piratage de lignes téléphoniques). C'est un courrier électronique qui vous demande, souvent pour des raisons de sécurité ou pour vous faire bénéficier de remboursement… de vous connecter 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'accroche peut aussi se faire par téléphone ou SMS, il consiste à vous faire appeler un numéro de téléphone ou envoyer un SMS. On parle alors de « vishing » et de « smishing ».

RÉAGIR À UNE TENTATIVE DE PHISHING

- **N'utilisez jamais le lien figurant** 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 SMISHING

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 mis en place par les principaux opérateurs français : plus d'informations sur www.33700-spam-sms.fr

5

Je contacte ma banque en cas de doute

Vous avez un doute sur le site (ou numéro de téléphone) ?

Si vous avez fourni vos codes d'accès de banque à distance, contactez immédiatement votre banque aux coordonnées habituelles pour lui signaler (n'utilisez pas celles du message que vous venez de recevoir). Sinon, vous risquez que les pirates accèdent à vos comptes à distance et procèdent à des virements ou, en récupérant vos codes BIC et IBAN, mettent en place des prélèvements SEPA.

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

Plus d'infos sur la sécurité informatique sur http://surfez-intelligent.dgmic.culture.gouv.fr .

Pour signaler un site ou un courrier d'escroquerie sur www.internet-signalement.gouv.fr et www.signal-spam.fr.

6

Je consulte régulièrement mon compte

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

Vérifiez le contenu de votre relevé de compte dès sa réception notamment avec les talons des chèques émis et les facturettes de carte.

Connectez-vous au moins une fois par semaine sur le site de votre banque à distance.

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.

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 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**. Suite à une usurpation d'identité, une ligne téléphonique pourrait être détournée et être utilisée pour effectuer des tentatives de fraudes bancaires sur vos comptes.

9

Je protège mon matériel

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

Vous devez lutter contre les logiciels malveillants (malwares) de tous types. Ces programmes nocifs s'introduisent sur les ordinateurs ou autres supports numériques comme les tablettes et smartphones. Il peut s'agir de :

- **spyware** : logiciel espion qui collecte les données personnelles et les envoie à un tiers,
- **keylogger** : logiciel spécialisé pour espionner les frappes au clavier, il peut recueillir les mots de passe, les codes de carte bancaires, etc.,
- **backdoor** : logiciel qui permet au pirate de prendre le contrôle de l'ordinateur...

En cas de perte ou de vol d'un terminal (tablette, ordinateur, téléphone...), 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 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 (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 avoir un virus sur votre ordinateur, lancez l'antivirus pour nettoyer l'ordinateur puis contactez votre agence pour demander de nouveaux codes d'accès.
- N'utilisez pas l'équipement dont vous ne maîtrisez pas le niveau de sécurité (cybercafé, libre-service…).
- Ne téléchargez que les programmes et contenus (photos, vidéos, sonneries, thèmes pour mobile et jeux) provenant d'une source fiable.

10

Je sécurise mes connexions

- Choisissez un fournisseur d'accès internet reconnu et suivez ses conseils de sécurité.
- Vérifiez la présence de **https** (« s » pour secure) **devant l'adresse du site**, icône d'une clé ou d'un cadenas dans la fenêtre du navigateur Internet.
- Contrôlez qu'aucune autre fenêtre internet n'est ouverte, **tapez vous-même l'adresse exacte fournie par la banque**.
- 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 » et effacez l'historique dès que vous avez fini.
- Si vous avez supprimé des documents, n'oubliez pas d'effacer le contenu de 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
10 RÉFLEXES SÉCURITÉ

1. Je consulte régulièrement les consignes de sécurité de ma banque
2. Je choisis avec soin mon mot de passe
3. Je garde secrets mes codes d'accès
4. Je ne me connecte jamais à partir d'un 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