A+ A-

Opérations bancaires à distance : comment vous protéger des risques de fraude ?

Par **Bercy Infos < https://economie.gouv.fr/entreprises/bercy-infos-qui-sommes-nous>** , le 20/10/2022 - **Droits et protection sur internet**

Faux sites internet de banques, mails frauduleux envoyés soi-disant par votre conseiller bancaire, comptes bancaires piratés...les fraudes aux opérations bancaires sont très répandues. Même si les banques ont des systèmes de protection de plus en plus performants, en tant que client de la banque, votre rôle est essentiel pour utiliser vos moyens de paiement et vos services bancaires à distance de manière sécurisée. On vous explique à quoi vous devez faire particulièrement attention !

Via son site service **lesclesdelabanque.com < https://www.lesclesdelabanque.com/particulier/>** , la **Fédération bancaire française (FBF) < http://www.fbf.fr/>** met à disposition du grand public des informations simples et pédagogiques pour comprendre les mécanismes bancaires et les utiliser au mieux. Retrouvez ici ses conseils pour utiliser vos services bancaires à distance en toute sécurité !

Consultez régulièrement les consignes de sécurité de votre banque

Même si vous pensez peut-être ne pas être concerné, ne négligez pas les informations de sécurité qui vous sont envoyées par votre banque, ou qui sont publiées sur son site internet !

Consultez régulièrement ces informations qui vous rappelleront les grands principes de sécurité à suivre pour assurer les sécurité de vos données personnelles et bancaires.

Choisissez un mot de passe sécurisé pour accéder à vos services bancaires en ligne

Comme pour vos autres démarches en ligne, il est essentiel que le mot de passe qui vous sert à vous connecter au site internet de votre banque (ou son application mobile) soit particulièrement sécurisé !

À ce titre, nous vous conseillons de lire notre article dédié : **Comment créer un mot de passe sécurisé et simple à retenir ?**

Surtout, **réservez un mot de passe dédié à votre seule banque à distance !** N'utilisez pas ce mot de passe pour d'autres utilisations (par exemple pour votre messagerie, ou pour vous identifier à d'autre sites internet, etc.).

Ne communiquez jamais vos codes d'accès au site de votre banque

Il s'agit d'une règle importante : **ne communiquez jamais votre identifiant et surtout votre mot de passe**, et cela même à votre banque ! Votre banque ne vous le demandera jamais. C'est justement l'une des techniques des fraudeurs, se faire passer pour votre banque afin que vous lui communiquiez vos données d'accès.

Autres conseils utiles :

- **ne gardez pas vos codes d'accès en mémoire** sur votre ordinateur, votre téléphone ou votre tablette
- si vous utilisez un équipement qui n'est pas le vôtre, **n'activez pas la fonction d'enregistrement automatique du mot de passe** et déconnectez-vous à la fin de votre utilisation.

Ne vous connectez pas au site de votre banque à partir d'un courriel ou sms

Les courriels ou les sms sont très souvent utilisés par les fraudeurs pour pirater des données. C'est ce que l'on appelle le phishing ou l'hameçonnage.

Concrètement, cette technique d'usurpation prend souvent la forme d'un courrier électronique ou d'un sms utilisant l'identité et/ou l'identité visuelle de votre banque, et qui vous demande (souvent pour des raisons de sécurité ou pour vous faire bénéficier de remboursement) de vous connecter au site de votre banque (mais cela peut concerner d'autres organismes). Le lien conduit en réalité vers un site pirate destiné à récupérer vos données personnelles et bancaires.

Pour vous prémunir contre ce risque, le réflexe de base est de ne j**amais vous connecter au site de votre banque ou à votre application mobile via un lien qui vous a été envoyé par courriel ou par sms !** En cas de doute, contactez directement votre banque par vos canaux habituels (sans utiliser les liens courriels ou sms).

Pour en savoir plus sur ce sujet du phishing, nous vous conseillons de lire notre article dédié : **Comment se prémunir contre les risque de phishing ?**

Sécurisez votre matériel informatique

Il s'agit d'un conseil valable pour assurer votre sécurité numérique en général, mais disposer d'un équipement informatique efficace et mis à jour régulièrement est un élément clé pour vous protéger d'éventuelles cyberattaques qui pourraient cibler plus spécifiquement vos opérations bancaires.

Quelques conseils sont à mettre en oeuvre :

- **Mettez à jour régulièrement vos équipements** : téléphone portable, tablette, ordinateur portable, etc.
- **Utilisez un anti-virus et un pare-feu** : et veillez également à les mettre à jour régulièrement.
- **Sécurisez votre accès au wifi** : configurez votre wifi personnel, a minima avec une clé WEP et idéalement avec une clé WPA 2 qui est plus sécurisée. Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur Internet ou accédez directement aux paramètres de votre wifi depuis votre compte personnel en ligne auprès de votre fournisseur d'accès. Plus généralement, ne vous connectez pas sur un wifi non sécurisé.
- **Verrouillez l'accès à votre profil utilisateur** : par un code ou mot de passe, afin de protéger vos documents. Sauvegardez régulièrement vos fichiers.
- **N'effectuez aucune opération bancaire à distance (connexion, virement, opposition ,etc...) si vous pensez avoir un virus sur votre ordinateur** : le réflexe est alors de lancer votre antivirus pour nettoyer votre terminal puis de contacter votre agence pour demander de nouveaux codes d'accès.

Sécurisez vos connexions

Là aussi, il s'agit de conseils de sécurité qui vous protègeront dans toutes vos activités en ligne, mais qui peuvent s'avérer particulièrement utiles pour protéger vos opérations bancaires.

- Ne consultez pas votre espace personnel sur le site internet de votre banque depuis un ordinateur qui n'est pas le vôtre ou via un WIFI public.
- **Même si vous consultez le site internet de votre banque depuis votre réseau WIFI** personnel, veillez bien à ce qu'il soit sécurisé : configurez votre WIFI personnel, a minima avec une clé WEP et idéalement avec une clé WPA 2 qui est plus sécurisée. Pour basculer vers cette dernière, saisissez « 192.168.1.1 » sur la barre d'adresses de votre navigateur Internet ou accédez directement aux paramètres de votre WIFI depuis votre compte personnel en ligne auprès de votre fournisseur d'accès.
- Lorsque vous naviquez sur le web, et notamment lorsque vous vous connectez au site internet de votre banque, **vérifiez la présence de https** (« s » pour *secure*) devant l'adresse du site, ainsi que de l'icône d'une clé ou d'un cadenas dans la fenêtre du navigateur internet.
- Si au cours de votre navigation vous avez téléchargé des documents, comme des relevés bancaires par exemple, veillez à bien les supprimer à la fin de votre utilisation.

Soyez également attentif à votre téléphone mobile

De plus en plus de clients utilisent leur téléphone mobile pour accéder à leurs services bancaires et/ou pour réaliser des achats en ligne qui sont validés via un code SMS envoyé de leur banque. Le téléphone est donc devenu, au même titre que les ordinateurs ou tablettes, une cible pour les pirates.

Soyez donc particulièrement vigilant, notamment dans les cas suivants :

- Si vous recevez un SMS de sécurité alors que **vous n'êtes pas en train de réaliser une opération bancaire sensible ou un achat en ligne**.
- Si vous constatez un dysfonctionnement sur votre ligne téléphonique : cela peut parfois cacher une usurpation d'identité lors de laquelle votre ligne téléphonique est détournée pour effectuer des tentatives de fraudes bancaires sur vos comptes. Dans ce cas, contactez votre opérateur téléphonique.

Consultez régulièrement vos comptes bancaires

Il s'agit d'un conseil de bon sens mais qui est indispensable pour détecter rapidement d'éventuelles anomalies : **consultez régulièrement votre compte en banque**. A minima, au moins une fois par semaine.

Au moindre doute : contactez votre banque !

En cas de doute sur une opération, n'attendez pas, **contactez votre banque par vos canaux habituels**. Cette dernière pourra effectuer les vérifications nécessaires et vous indiquer la marche à suivre si nécessaire.

À savoir

Retrouvez dans le détail tous les conseils pour effectuer vos opérations bancaires à distance en toute sécurité, en consultant le guide de la Fédération bancaire française (FBF), intitulé « **Banque à distance : les 10 réflexes de sécurité » [PDF ; 420Ko] < https://lesclesdelabanque.com/web/Cdb/Particuliers/Content.nsf/DocumentsByIDWeb/9W8AGL/$File/Guide-securite-04-banque-a-distance.pdf?v=1666263297>**

En savoir plus sur la sécurité sur internet

Comment protéger ses données personnelles ?
Objets connectés : que faut-il savoir pour bien se protéger ?
Démarches en ligne : attention aux faux sites administratifs payants
Attention aux faux courriels et appels qui se font passer pour l'administration
Comment créer un mot de passe sécurisé et simple à retenir ?
Comment assurer sa sécurité numérique ?
Dix règles pour vous prémunir des risques de piratage de votre ordinateur
Usurpation d'identité, comment s'en protéger ?

En savoir plus sur la sécurité des opérations bancaires

Vous pouvez consulter les publications sur la sécurité des opérations bancaires (ainsi que sur d'autres sujets), sur le site **lesclesdelabanque.com < https://www.lesclesdelabanque.com/particulier/>** , service de la Fédération bancaire française (FBF) et notamment le guide « **Fraude aux opérations bancaires » [PDF ; 1 Mo] < https://www.lesclesdelabanque.com/web/Cdb/Particuliers/Content.nsf/DocumentsByIDWeb/6WNHMA/$File/Guide-HS-fraudes-remboursement.pdf?v=1666263297>** , publié en janvier 2021.

Thématiques : **Droits et protection sur internet**

Ce sujet vous intéresse ? Chaque mardi avec la lettre Bercy infos Particuliers, ne manquez aucune info pratique sur vos droits et obligations en matière de fiscalité, épargne, consommation …

exemple : nom.prenom@domaine.com Je m'al

Je consens à ce que mon adresse email soit utilisée afin de recev
de Bercy infos. Consulter notre politique de confidentiali

Partager la page