RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FINANCES PUBLIQUES

Foire aux questions (FAQ) 27/02/2026

Accès illégitimes au fichier national des comptes bancaires FICOBA

Le fichier national des comptes bancaires FICOBA c'est quoi ?
FICOBA liste tous les comptes bancaires ouverts en France, pour plus d'informations : **https://www.cnil.fr/fr/cnil-direct/question/ficoba-cest-quoi**

Pourquoi j'ai reçu un message de la Direction générale des Finances Publiques ?

Des investigations menées par la Direction Générale des Finances publiques (DGFiP) ont révélé que des consultations ont été effectuées illégalement sur le fichier national des comptes bancaires (FICOBA) tenu par la DGFiP entre le 28 janvier et le 13 Février.

Une consultation illégale ne signifie pas une intervention ou une fraude sur un compte bancaire, mais simplement l'accès à l'information. La DGFiP a pour obligation d'informer dès qu'une consultation semble frauduleuse, conformément à l'article 34 du règlement général sur la protection des données (RGPD).

Est-ce que je suis concerné par les consultations qui ont été effectuées illégalement sur le fichier national des comptes bancaires (FICOBA) ?

Tous les usagers concernés ont reçu ou vont recevoir dans les jours qui viennent un message d'information directement par la Direction générale des Finances publiques, par courriel ou par courrier lorsque nous ne disposons pas de l'adresse mail.

Si vous ne recevez pas de courriel ou de courrier de la DGFiP, c'est que vous n'êtes pas concernés.

La consultation illégitime a concerné moins de 1 % des coordonnées bancaires contenues dans le fichier.

Quelles données ont pu être consultées ?

Il s'agit de votre état-civil, de votre adresse postale et de vos coordonnées bancaires.

Les opérations réalisées sur vos comptes et le montant du solde ne figurent pas sur le fichier FICOBA, ils n'ont donc pas été consultés.

Il n'y a aucun mot de passe personnel contenu dans le fichier FICOBA. Vos accès aux applications bancaires ou à votre espace Finances publiques du site impots.gouv.fr ne sont pas compromis.

Est-ce que je dois changer de compte bancaire/banque ?

Non. Il n'est pas nécessaire de changer de coordonnées bancaires.

Quel est l'impact de ces consultations sur mon espace Finances publiques et mes prélèvements (prélèvements à la source, prélèvements mensuels et à l'échéance) ?

Aucun.

Votre identifiant fiscal et l'accès à votre espace Finances publiques ne sont pas compromis. Vous pouvez continuer à utiliser sans crainte votre espace pour bénéficier des services en ligne proposés par la DGFiP.

Les prélèvements qui ont été autorisés continuent de s'effectuer sur les coordonnées bancaires qui ont été communiquées. Il n'est pas utile de les modifier.

Quelles peuvent être les conséquences de ces consultations malveillantes ?

Les conséquences portent principalement sur de possibles tentatives d'escroqueries par l'intermédiaire de messages (« hameçonnage ») ou d'appels frauduleux (ex : fraudes par manipulation notamment au faux conseiller bancaire).

Plus marginalement, les personnes concernées par ces consultations malveillantes peuvent être victimes de tentatives d'usurpation d'identité ou de prélèvements bancaires non autorisés. Pour cela, il faut également la copie de vos papiers d'identité.

L'accès à un IBAN n'expose pas nécessairement à une fraude bancaire. Le risque est souvent limité. Un malfaiteur peut effectivement l'utiliser pour tenter de prélever un compte, mais il doit pour cela créer un faux mandat de prélèvement, ce qui nécessite d'être enregistré auprès d'une banque en tant qu'émetteur de prélèvements.

Que dois-je faire si je suis concerné ?

De manière générale, il convient d'être particulièrement méfiant face à tout appel téléphonique ou message (mail, SMS, messageries instantanées, réseaux sociaux…) de personnes ou d'organismes qui prétendraient vous connaître à partir des informations dérobées et vous contacteraient dans le but de vous soutirer des informations confidentielles (codes, mots de passe, numéros de carte bancaire, copies de documents d'identité…), vous faire valider des opérations bancaires (faux conseiller bancaire notamment) ou demander votre mot de passe pour accéder à votre espace Finances publiques.

L'administration fiscale ne vous demande jamais vos identifiants ou votre numéro de carte bancaire par message.

Prenez toujours le temps de vérifier les informations par vous-même, surtout quand on vous incite à réagir rapidement. Au moindre doute, il est préférable de ne pas répondre directement et de ne rien faire sans rappeler vous-même au préalable

l'établissement concerné à partir des coordonnées publiées sur les annuaires (ne pas utiliser la fonction « rappel » du téléphone).

Quelle attitude adopter ?

Il est recommandé de :

- Prévenir votre établissement bancaire que vous avez été informés par la DGFIP d'une consultation illégale de vos données FICOBA. La DGFiP prévient les établissements bancaires concernés de son côté ;
- Consultez régulièrement votre compte pour détecter tout incident ou anomalie. Connectez-vous au moins 1 fois par semaine à votre espace de banque à distance via le site ou l'application mobile de votre banque ;
- Vérifiez les opérations inscrites à votre compte, en cas de doute ou si vous n'êtes pas à l'origine d'une opération prévenez immédiatement votre banque. L'article L133-24 du Code monétaire et financier dispose en effet que l'utilisateur de services de paiement signale, sans tarder, à son prestataire de services de paiement une opération de paiement non autorisée ou mal exécutée et au plus tard dans les treize mois suivant la date de débit;
- Par mesure de précaution, nous vous conseillons de conserver toutes les preuves (messages, adresse du site, captures d'écran…) si vous suspectez une utilisation frauduleuse de vos données. Le site https://www.cybermalveillance.gouv.fr/ est disponible pour plus d'informations ;
- Que vous soyez particulier, entrepreneur, entreprise, jamais votre banquier ne vous demandera vos codes, identifiants, mots de passe. Que cela soit par téléphone, à distance ou physiquement. Il n'en a pas besoin. Si quelqu'un vous contacte et cherche à les obtenir, mettez fin à l'échange et contactez votre banque par un moyen sécurisé.

Pour toute autre question, vous pouvez contacter notre délégué à la protection des données (DPD) : le-delegue-a-la-protection-des-donnees-personnelles@finances.gouv.fr

Que faire si je constate une usurpation de mon identité ?

La seule consultation de vos coordonnées bancaires ou de votre état civil ne signifie pas nécessairement que votre identité est usurpée.

Cette information sur l'usurpation d'identité vous a été donnée à titre indicatif et préventif, au cas où une tentative de fraude vous concernerait, pour vous simplifier les démarches. Si vous ne constatez pas de mouvements suspects, il n'est pas nécessaire de procéder à une demande d'accès aux comptes.

Si vous recevez des demandes de prélèvement ou d'achat dont vous n'êtes pas à l'origine, vous pouvez faire une demande d'accès au fichier FICOBA et déposer

plainte, notamment en cas d'usurpation d'identité.

Est-ce que je dois demander si un nouveau compte bancaire a été créé à mon nom ?

En l'absence de mouvements suspects, il n'est pas nécessaire de procéder à une demande FICOBA. En effet, consultation illégale ne signifie pas intervention sur le compte.

Mes données personnelles divulguées ont été utilisées frauduleusement, que dois-je faire ?

Vous devez conserver toutes les preuves (messages, adresse du site web, captures d'écran…) et déposer plainte au commissariat de police ou à la brigade de gendarmerie dont vous dépendez.

Quels sont les conseils de la Banque de France ?

Les données divulguées issues du fichier FICOBA ne permettent pas d'accéder aux soldes des comptes et ne suffisent pas à la réalisation d'opérations bancaires. Il est toutefois recommandé de faire preuve d'une grande vigilance et d'adopter les bons réflexes afin de se protéger contre les risques de fraude en cas de fuite de données personnelles. Pour en savoir plus sur le vol de données bancaires et ses conséquences, vous pouvez consulter le site internet de la Banque de France : Vous avez été victime du vol de vos données personnelles, la Banque de France vous aide | Banque de France.

Par ailleurs, l'ensemble de vos demandes auprès de la Banque de France peut être réalisé directement en ligne en créant votre espace personnel à l'adresse suivante Vos demandes en ligne | Banque de France. Il est rappelé qu'aucune information concernant l'existence ou non d'un éventuel fichage ne peut être communiquée par téléphone.