

Piratage du fichier national des comptes bancaires Ficoba

Quels risques et comment
s'en protéger ?



CONSEILLER
NUMÉRIQUE

Accès illégitime au FICOBA

Le Fichier National des Comptes Bancaires et Assimilés (FICOBA)



Que s'est-il passé ?

Le 18 février 2026, le ministère de l'Économie et des Finances a révélé un accès non autorisé au FICOBA.

Cet incident a compromis les données de **1,2 million de comptes** gérés par la DGFIP.



Qu'est-ce que le FICOBA ?

Le Fichier National des Comptes Bancaires et Assimilés (FICOBA) est une base de données administrative gérée par l'administration fiscale.

Son rôle est de recenser l'ouverture, la modification et la clôture de tous les comptes ouverts en France.



Ce que le FICOBA contient :

- **Identité civile**
Nom, prénom, date et lieu de naissance, adresse.
- **Coordonnées bancaires**
IBAN, RIB, nom de la banque, type de compte.
- **Identifiant fiscal**
- **Vie du compte**
Dates d'ouverture, de modification ou de clôture.



Ce qu'il ne contient PAS :

- **Le solde de vos comptes**
- **Le détail de vos opérations**
- **Vos codes secrets ou identifiants**

Suis-je concerné(e) ?

Si vous êtes concerné(e) :

Vous recevrez un message officiel de la Direction générale des Finances publiques par courriel ou par courrier si vous ne disposez pas d'adresse mail.

Direction générale des Finances publiques <ne-pas-repondre@dgfip.finances.gouv.fr>

À :



Consultation illégale de vos informations bancaires

Bonjour

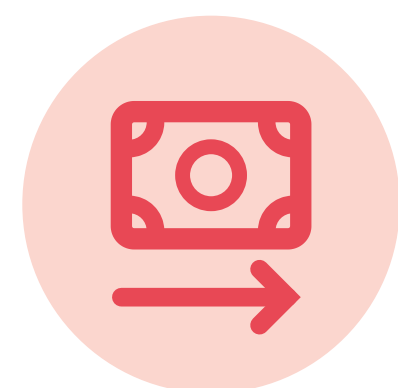
Des investigations menées par la Direction générale des Finances publiques (DGFIP) ont révélé que des consultations ont été effectuées illégalement sur le fichier national des comptes bancaires (FICOBA) entre le 28 janvier et le 13 février. Vous recevez ce message car vous êtes malheureusement concerné(e) par cet acte de malveillance.

Des mesures ont immédiatement été prises pour interrompre cette violation des données. Nous avons informé les établissements bancaires français de cet incident, déposé plainte et informé la CNIL.

Quelles sont les données susceptibles d'avoir été consultées ? Votre état-civil, votre adresse postale, vos coordonnées bancaires ou votre identifiant fiscal. Important à noter : le mot de passe de

Les risques

Que peut faire un pirate avec vos données bancaires et personnelles ?



Prélèvements SEPA frauduleux

Les fraudeurs utilisent votre IBAN pour mettre en place des prélèvements automatiques. Ils commencent souvent par de petits montants (quelques euros) noyés dans vos relevés pour passer inaperçus avant d'augmenter la somme.



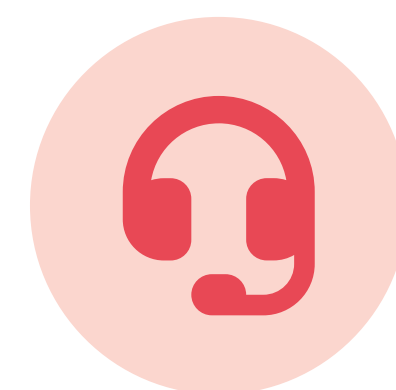
Usurpation d'identité

Avec vos données civiles (nom, adresse, date de naissance) et votre RIB, des escrocs peuvent souscrire à des abonnements à votre nom, ou effectuer des achats sur des sites de e-commerce peu sécurisés.



Phishing ciblé

Contrairement aux spams classiques, ces mails ou SMS utilisent vos vraies informations pour paraître crédibles. Ils vous incitent à cliquer sur un lien malveillant ou à faire un virement "urgent" en se faisant passer pour une administration.



Arnaque au faux conseiller

Un escroc vous appelle en se faisant passer pour le service fraude de votre banque. Il cite votre adresse et votre banque (qu'il connaît grâce à la fuite) pour gagner votre confiance et vous faire valider des opérations frauduleuses.

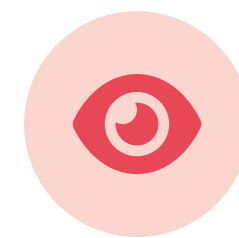
Comment se protéger ?

Les réflexes essentiels pour sécuriser vos comptes



Votre vigilance est la clé

Face à la fuite de données,
c'est votre comportement qui
empêchera les escrocs
d'exploiter vos données.



Surveillez vos comptes régulièrement

Le moindre débit inconnu,
même de quelques euros,
doit être signalé.



Gardez vos codes secrets

Le moindre débit inconnu,
même de quelques euros,
doit être signalé.



Ne cliquez sur aucun lien

Mails, SMS : ne suivez jamais
les liens. Connectez-vous
toujours en tapant vous-
même l'adresse du site
officiel ou via l'application.



Mettez en place une liste blanche

Faites la demande auprès de
votre banque, seuls les
organismes que vous validez
peuvent vous prélever.

Que faire en cas de fraude ?

Les étapes à suivre immédiatement si vous constatez une anomalie



Contactez votre banque

Appelez immédiatement le service d'opposition (disponible 24h/24).

Faites bloquer les moyens de paiement concernés et contestez les prélèvements frauduleux.



Sécurisez vos accès

Si vous avez cliqué sur un lien ou donné un mot de passe, changez-le immédiatement.

Activez la double authentification (2FA) partout où c'est possible.



Conservez les preuves

Ne supprimez rien. Faites des captures d'écran des SMS, emails, ou des opérations bancaires suspectes. Notez les URL des sites frauduleux.



Déposez plainte

Rendez-vous à la gendarmerie ou au commissariat de police.

Pour les fraudes à la carte bancaire, vous pouvez utiliser la plateforme en ligne **Perceval** (service-public.gouv.fr).



Vous avez des questions ?

A bientôt !



**CONSEILLER
NUMÉRIQUE**



Attribution :

Pas d'Utilisation Commerciale
Pas de Modification 4.0 International

Création : Eric Antier, Conseiller numérique - 2026

Sources :

<https://presse.economie.gouv.fr/acces-illegitimes-au-fichier-national-des-comptes-bancaires-ficoba/>
<https://www.impots.gouv.fr/actualite/acces-illegitimes-au-fichier-national-des-comptes-bancaires-ficoba>