CONSEILS EN CAS DE PIRATAGE DE VOS DONNEES PERSONNELLES

Mercredi 12 et jeudi 13 août 2026, un acteur malveillant a revendiqué des accès illégitimes au système d'information de la Direction générale des Finances publiques (DGFiP), intervenus en juin et juillet 2026.

Depuis l'annonce de la cyberattaque contre le fisc, une seule question circule : suis-je concerné ? La réponse tient en deux temps. La DGFiP contacte individuellement chaque personne touchée à partir de la semaine du 18 août. Et il n'existe, à ce jour, aucun moyen de le vérifier soi-même. Ce vide est déjà exploité par des escrocs.

La Direction générale des finances publiques a confirmé le 14 août que des données fiscales et cadastrales concernant 678 000 particuliers et professionnels ont pu être consultées et extraites. L'intrusion remonte à fin juin, par usurpation des identifiants d'un agent et d'un tiers habilité.

Aucun critère public ne permet de deviner si votre dossier fait partie du lot : ni votre département, ni votre tranche de revenus, ni l'ancienneté de votre compte. Les investigations se poursuivent avec l'ANSSI pour déterminer précisément l'étendue de la fuite, et le parquet de Paris a ouvert une enquête.

De l'intrusion à l'information des contribuables

DATE	ÉVÉNEMENT
Fin juin 2026	Intrusion via les identifiants usurpés d'un agent et d'un tiers habilité
Fin juin à juillet	La DGFiP détecte une activité suspecte sur les comptes et coupe les accès
12 août	Un pirate revendique publiquement 678 438 lignes de données fiscales
14 août	La DGFiP confirme, notifie la CNIL et dépose plainte
Semaine du 18 août	Début de l'information individuelle des personnes concernées

Chronologie reconstituée à partir des communications de la DGFiP et de la revendication publique.

Ce qui a fuité, et ce qui n'a pas bougé

La distinction est essentielle pour mesurer le risque réel. Les données exposées sont administratives et fiscales, pas bancaires.

Les investigations approfondies conduites depuis le 12 août 2026 ont permis d'établir que, préalablement à leur interruption, ces accès avaient été utilisés pour consulter et extraire certaines données concernant un total de 678 000 particuliers et professionnels, notamment des données fiscales telles que le revenu fiscal de référence, le quotient familial ou le taux de prélèvement à la source, et en ce qui concerne les entreprises, des données telles que leur raison sociale ou leur SIREN.

Des données cadastrales relatives aux adresses et aux surfaces de biens immobiliers ont également été consultées.

Dès l'identification de ces vols de données, la DGFIP a saisi la CNIL. Les espaces Finances publiques des usagers particuliers et professionnels n'ont pas été compromis. Les identifiants et les mots de passe des particuliers et des professionnels n'ont pas été compromis.

Données exposées et données préservées

EXPOSÉ	PRÉSERVÉ
Identité, date et lieu de naissance	Identifiants et mots de passe
Adresse postale, téléphone, courriel	Espace personnel impots.gouv.fr
Revenu fiscal de référence, taux de prélèvement	Coordonnées bancaires
Situation familiale, personnes à charge	Moyens de paiement

D'après les éléments communiqués par la DGFiP et l'échantillon publié par l'auteur de la revendication.

Personne ne peut donc prélever sur votre compte avec ce qui a été volé. Le risque est indirect : ces informations rendent crédible un contact frauduleux

La DGFiP a notifié l'incident à la Commission nationale de l'informatique et des libertés et déposé plainte. De nouveaux éléments seront communiqués au fil des investigations : le périmètre annoncé aujourd'hui peut encore évoluer.

Pourquoi cette notification piratage va créer une deuxième vague de risques ,

La DGFiP a l'obligation légale d'informer individuellement chaque personne concernée (article 34 du RGPD). Cette communication doit décrire la nature de la violation, les données exposées, les conséquences possibles et les mesures prises.

Mais les cybercriminels connaissent parfaitement ce mécanisme. Ils vont exploiter la fenêtre de quelques jours entre l'annonce publique et la réception effective des notifications pour envoyer de faux courriers et de faux emails imitant la DGFiP. Leur objectif : vous pousser à cliquer sur un lien, communiquer vos identifiants ou valider une opération bancaire.

C'est ce que les spécialistes appellent le « phishing de rebond » : une vraie fuite de données sert de prétexte à une seconde attaque, encore plus ciblée.

Les 4 critères pour reconnaître la vraie notification de la DGFiP

1. Le vrai courrier ne contient JAMAIS de lien cliquable urgent. La DGFiP ne vous demandera pas de « vérifier votre compte immédiatement » via un bouton ou un lien. Si un message vous presse de cliquer, c'est une arnaque.

2. Le vrai courrier ne demande AUCUNE information personnelle en retour. Ni mot de passe, ni numéro de carte bancaire, ni code reçu par SMS. La notification est purement informative : elle vous alerte et vous conseille, elle ne vous demande rien.

3. Le vrai courrier mentionne des éléments vérifiables. Le message rappelle brièvement les faits, puis énumère les informations susceptibles d'avoir été consultées.

Y figurent l'identifiant fiscal, l'état civil, les coordonnées et la situation fiscale. S'y ajoute un élément qui n'avait pas été détaillé jusqu'ici : la liste des messages échangés avec la DGFiP via la messagerie d'impots.gouv.fr. Un historique de conversation qui donne à un escroc de quoi rendre une prise de contact troublante de vraisemblance.

L'administration précise en revanche ce qui n'a pas bougé. Les déclarations et les avis d'impôts sont restés préservés, tout comme les accès aux espaces personnels sur impots.gouv.fr. Le texte se conclut par l'annonce de « mesures de sécurisation supplémentaires, engagées sans délai », puis par des excuses, signées de la direction générale des Finances publiques.

4. Le vrai courrier ne propose AUCUNE « indemnisation » ni « remboursement ». Tout message évoquant une compensation financière liée au piratage est frauduleux. L'administration ne verse aucune indemnité dans ce cadre.

Reconnaître le courriel authentique de la DGFiP

CRITÈRE	LE MESSAGE OFFICIEL
Liens	Aucun lien d'accès aux services en ligne
Expéditeur	Une adresse en dgfip.finances.gouv.fr
Informations demandées	Aucune donnée confidentielle réclamée
Action attendue	Aucune validation d'opération, aucun mot de passe

D'après les précisions communiquées par la DGFiP et ses consignes de sécurité publiées sur impots.gouv.fr.

Les 5 gestes à adopter dès réception de la notification piratage

Vérifiez vos mandats de prélèvement. Connectez-vous à votre espace bancaire en ligne et consultez la liste des créanciers autorisés.

Si un organisme inconnu y figure, contestez le mandat immédiatement. Mieux encore : demandez à votre banque de mettre en place une liste blanche de créanciers autorisés. Tout prélèvement émanant d'un créancier absent de cette liste sera automatiquement rejeté. C'est la protection la plus efficace et pourtant la moins connue.

Surveillez vos comptes chaque semaine. Pendant les trois à six prochains mois, soyez particulièrement attentif aux petits montants inhabituels. Les fraudeurs testent souvent avec des prélèvements de quelques euros avant de passer à des sommes plus importantes.

Vérifiez qu'aucun compte n'a été ouvert à votre nom. Connectez-vous sur impots.gouv.fr, rubrique « Autres services », puis « Accéder au fichier Ficoba ». Vous verrez la liste de tous les comptes bancaires ouverts à votre nom en France.
https://www.service-public.gouv.fr/particuliers/vosdroits/R64101

Signalez tout prélèvement suspect à votre banque sans attendre. En cas d'opération frauduleuse constatée, la banque doit rembourser dès qu'elle est informée, dans la limite de 13 mois après le débit.

Si vous êtes victime de cybermalveillance (rançongiciels, piratage, virus, faux ordres de virement…), vous pouvez réaliser un diagnostic en ligne (17 Cyber) pour identifier la nature de la cybermenace, et si vous le souhaitez, être accompagné via le tchat par un policier ou un gendarme.
https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/17-cyber-dispositif-cybersecurite

Victime de fraude à la carte bancaire sur internet, le service Perceval simplifie la démarche de signalement.
https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/signaler-fraude-carte-bancaire-perceval

Conservez toutes les preuves. Messages suspects, captures d'écran, relevés montrant des opérations douteuses. Ces éléments seront indispensables en cas de dépôt de plainte.

Sources : https://www.service-public.gouv.fr/