La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Hors Série n°01 / 2026

🚨 Fuites de données à la Direction Générale des Finances Publiques (DGFiP)

DIFFUSION LIBRE

Vous avez été nombreux à nous solliciter suite à vos préoccupations sur la fuite de données que touche la DGFiP. Suites aux investigations menées 👨‍⚖️ , un total de 678 000 particuliers et professionnels ont vu leurs données consultées ou extraites.
Voici ce qui serait extrait :

🔴 Données fiscales

Plus de 300 000 particuliers sont concernés par l'accès à des échanges entre contribuables et administration. Des informations fiscales sensibles ont pu être consultées ou extraites.

🟠 Données cadastrales

Plus de 400 00 particuliers et professionnels pourraient être concernés. Les informations portent notamment sur des données relatives aux biens immobiliers, comme les adresses et surfaces.

🟡 Données liées aux successions

Un troisième accès, détecté le 17 août, concernait un portail lié aux recherches successorales. Cet accès a rapidement été coupé.

🔎 Pourquoi faut-il être particulièrement vigilant ?

Un cybercriminel n'a pas forcément besoin de votre mot de passe ou de votre carte bancaire. Avec un nom, une adresse, des informations fiscales ou patrimoniales, il peut construire un scénario beaucoup plus crédible :

📩 « Votre dossier fiscal nécessite une vérification. »
📱 « Une anomalie a été détectée sur votre compte. »

🏦 « Votre déclaration entraîne un remboursement 💵 de 1 247 €. »

🏠 « Une opération concernant votre bien immobilier nécessite votre validation. »

Et lorsque le message contient déjà plusieurs informations exactes sur vous, la confiance augmente… et le piège devient plus difficile à détecter 🎣.

Les bons réflexes

- ✅ Ne cliquez pas sur un lien reçu par SMS ou courriel pour accéder à votre espace fiscal.
- ✅ Connectez-vous directement en saisissant vous-même l'adresse officielle du Service.
- ✅ Ne communiquez jamais votre mot de passe, code de validation ou coordonnées bancaires à la suite d'un message inattendu.
- ✅ Activez la double authentification lorsqu'elle est disponible.
- ✅ Utilisez des mots de passe uniques pour vos comptes importants.
- ✅ Soyez particulièrement méfiant face à un message contenant des informations personnelles précises.
- ✅ En cas de doute, contactez directement l'organisme concerné par un canal Officiel.

👉 **Une information exacte dans un message ne signifie pas que le message est authentique.**

+ D'INFO

Vous êtes victime ?

Appelez immédiatement le 📞 **17** ou 💻 contacter :

LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
https://17cyber.gouv.fr/

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

LA CNIL

Prévenir en cas de fuite de données personnelles, réelle ou supposée.

CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr

GRAND EST CYBERSECURITE

Assistance cyberattaque gratuite
Tel : 0 970 512 525
www.cybersecurite.grandest.fr

L'ANSSI

Assiste les entités essentielles et les entités importantes, fournit des guides
https://cyber.gouv.fr

THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.

Vous souhaitez joindre un Référent Cyber
de la Région de Gendarmerie du Grand-Est
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)

01010010 01001001 01010011 01000011 01001000