La Cyber-Lettre de la GENDARMERIE RÉGION GRAND EST

Mois 2026

Les fuites de données.

Quand vos informations prennent la porte sans prévenir

DIFFUSION LIBRE

Les fuites de données sont devenues l'un des risques numériques les plus fréquents pour les particuliers, entreprises et collectivités. Elles surviennent lorsqu'une base de données est volée, exposée par erreur ou publiée en ligne. Résultat : noms, adresses, mots de passe, IBAN, numéros de téléphone ou documents internes peuvent circuler entre cybercriminels.

Une fuite de données ne fait pas toujours de bruit mais ses conséquences, elles, se font entendre longtemps

🚨 Quelques cas concrets médiatisés

Ces dernières années, de nombreuses organisations ont été touchées :

- Enseignes commerciales victimes de vol de fichiers clients ;
- Plateformes en ligne exposant des millions d'identifiants ;
- Collectivités locales touchées après piratage ou mauvaise configuration serveur ;
- Professionnels de santé confrontés à la divulgation de dossiers sensibles.

Une seule fuite peut alimenter des campagnes de phishing, d'usurpation d'identité ou de fraude bancaire pendant plusieurs mois

⚠️ Quels sont les risques ?

Si vos données figurent dans une fuite, vous pouvez faire l'objet de :

- Tentatives d'escroqueries personnalisées par SMS, mail ou téléphone ;
- Réutilisation de vos mots de passe sur d'autres services ;
- Création de faux comptes à votre nom ;
- Chantage ou diffusion d'informations sensibles ;
- Atteinte à la réputation, en particulier d'une entreprise ou d'une collectivité.

Les cybercriminels aiment recycler : une ancienne fuite reste souvent exploitable

🎯 À retenir

Une fuite de données n'est pas seulement un problème informatique, c'est souvent le début d'autres attaques.

💡 Bonnes pratiques :

Pour les particuliers :

✔️ Utilisez un mot de passe complexe différent sur chaque site.
✔️ Activez l'authentification à deux facteurs (2FA).
✔️ Changez immédiatement un mot de passe compromis.
✔️ Vérifiez régulièrement si votre adresse mail apparaît dans une fuite.
✔️ Méfiez-vous des messages trop précis utilisant vos vraies informations.

Pour les entreprises et collectivités :

✔️ Limitez l'accès aux données sensibles.
✔️ Chiffrez les bases de données et sauvegardes.
✔️ Mettez à jour les systèmes et logiciels.
✔️ Sensibilisez les agents et salariés.
✔️ Préparez un plan de gestion de crise en cas de fuite.
✔️ Déclarez rapidement l'incident si nécessaire.

🚫 Pièges à éviter.

❌ Utiliser le même mot de passe partout.
❌ Ne pas ignorer une alerte de compromission.
❌ Envoyer des fichiers sensibles sans protection.

Penser : "Qui voudrait mes données ?"
👉 En cyber, tout se revend.

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

LE 33700

Transférer les SMS frauduleux au 33700. La plateforme de signalement.

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.

+ D'INFO

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

01010010 01001001 01010011 01000011 01001000