



La Cyber-Lettre de la **GENDARMERIE** **RÉGION GRAND EST**



Juillet 2026

Quand une fuite de données peut ouvrir la porte de votre domicile

**DIFFUSION
LIBRE**

Lorsqu'une fuite de données est évoquée, les premiers risques qui viennent à l'esprit sont généralement le phishing, l'usurpation d'identité ou encore le piratage de comptes. Pourtant, les conséquences peuvent dépasser le cadre du numérique et avoir un impact bien réel sur la sécurité des personnes et des biens.

Les récentes compromissions ayant touché plusieurs acteurs du tourisme et de la location de vacances illustrent parfaitement cette menace. Une simple base de données clients peut constituer une source d'informations particulièrement précieuse pour des individus malveillants. Parmi les données susceptibles d'être compromises figurent notamment :

- Les nom et prénom
- Les coordonnées (*adresse postale, e-mail et numéro de téléphone*)
- Les dates de séjour



Croisées avec d'autres informations librement accessibles sur Internet ou les réseaux sociaux, ces données peuvent permettre d'identifier les périodes d'absence d'un domicile. Un individu malveillant peut ainsi déduire qu'une famille sera absente pendant plusieurs jours, rendant la préparation d'un cambriolage plus aisée.

Les forces de l'ordre rappellent régulièrement que les cambrioleurs exploitent désormais des renseignements collectés en ligne. Publier une photo de son embarquement à l'aéroport, annoncer son départ en vacances sur les réseaux sociaux ou voir ses dates de séjour divulguées à la suite d'une fuite de données sont autant d'éléments qui peuvent être exploités.

Une fuite de données n'entraîne évidemment pas, à elle seule, un cambriolage. En revanche, elle peut fournir une information stratégique qui, une fois recoupée avec d'autres sources, facilite le repérage de cibles potentielles par des réseaux criminels organisés.

La protection des données personnelles constitue un enjeu de cybersécurité essentiel et également un levier essentiel de sécurité du quotidien.



Bonnes pratiques :

Vous venez d'apprendre qu'une entreprise s'est faite dérober ou a perdu vos données :

- ✓ Changez immédiatement votre mot de passe.
- ✓ Activez l'authentification multi-facteur
- ✓ Soyez vigilant aux SMS, appels et e-mails évoquant votre réservation.
- ✓ Évitez d'annoncer vos vacances en temps réel sur les réseaux sociaux.
- ✓ Demandez à un voisin de relever régulièrement votre courrier.
- ✓ Vous partez en vacances? Inscrivez vous au dispositif **Opération Tranquillité Vacances** proposé par la Gendarmerie et la Police



Pour vous inscrire au dispositif **OTV***, rendez-vous dans votre brigade de Gendarmerie, dans votre commissariat de Police ou par internet : <https://www.service-public.gouv.fr/>

* Certaines Polices Municipales peuvent participer à ce dispositif.

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