



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



Juin 2026



Escroquerie au péage en flux libre

Attention aux faux SMS



**DIFFUSION
LIBRE**

Les péages en flux libre  se déploient progressivement sur les autoroutes françaises. Plus de barrières, plus d'arrêt au guichet : les portiques détectent votre plaque et le paiement s'effectue en ligne après votre passage . Un système moderne, fluide... et malheureusement déjà exploité par des escrocs.

Depuis la mise en service du péage en flux libre sur l'Autoroute A79, puis sur l'Autoroute A13, de nombreux usagers reçoivent  :

- Des SMS indiquant un « *solde restant dû* »
- Un lien vers un site imitant parfaitement celui de l'exploitant
- Une demande de paiement immédiat sous peine de majoration

Il s'agit d'une campagne massive de phishing.

Même si plusieurs médias nationaux ont relayé ces escroqueries : Des automobilistes  ont payé pensant régulariser quelques euros... Résultat : ***données bancaires compromises, prélèvements frauduleux, voire revente d'informations personnelles sur des plateformes clandestines.***

Les messages reçus utilisent :

- L'urgence : Dernier rappel avant majoration
- La crédibilité visuelle : logo, couleurs officielles
- La confusion technologique : flux libre encore méconnu

Le péage en flux libre simplifie la circulation. Les escrocs exploitent surtout la nouveauté et la méconnaissance. La vigilance numérique devient un réflexe routier.



Bonne pratique :

- ✓ Ne cliquez jamais sur un lien reçu par SMS concernant un péage
- ✓ Rendez-vous directement sur le site officiel de votre concessionnaire
- ✓ Vérifiez l'adresse du site (orthographe, extension, https)
- ✓ Activez l'authentification forte sur vos services bancaires



Pièges à éviter.

- ✗ Cliquer sur un lien reçu sans vérification
- ✗ Payer dans la précipitation
- ✗ Enregistrer sa carte bancaire sur un site non vérifié
- ✗ Rappeler un numéro inconnu mentionné dans le SMS

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.



**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)

