La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Année 2025 – Hors Série n° 01

ALERTE PHISHING

Les professionnels de l'automobile ciblés !

DIFFUSION LIBRE

Depuis plusieurs mois, des escrocs ciblent les professionnels du Système d'Immatriculation des Véhicules (SIV) en usurpant l'identité de l'ANTS.

Ils envoient un courriel frauduleux du type demande@declaration-ants.com / habilitation@controleur-ants.com, dans lequel ils annoncent un prétendu contrôle de l'agence.

Un faux « agent » contacte ensuite la victime par téléphone et lui demande d'installer un logiciel de prise de contrôle à distance (*AnyDesk, TeamViewer, RustDesk*...).

Sous prétexte de vérifier ses démarches, il fait se connecter la victime au site de l'ANTS (***A**gence **N**ationale des **T**itres **S**écurisés*) et dérobe à son insu ses identifiants. Parfois, un faux rendez-vous sur place est fixé afin de crédibiliser la manœuvre.

Avec les identifiants volés, le fraudeur se reconnecte par la suite au compte du professionnel et émet massivement des certificats d'immatriculation 

(déclarations d'achats, cessions, ventes...).

💡 Bon à savoir :

Aucun service de l'État ne vous demandera par mail des informations relatives à votre habilitation ou votre agrément SIV.

Si vous avez cliqué sur un lien ou transmis vos données, contactez immédiatement votre référent SIV en préfecture ainsi que le 17 Cyber ou le CSIRT (Grand Est Cybersécurité) qui vous guideront sur les mesures et actions à entreprendre.

⚠ Ne tombez pas dans le piège !

- ✅ Ne répondez pas et ignorez le message ;
- ✅ Ne cliquez sur aucun lien suspect ;
- ✅ Ne communiquez jamais vos identifiants ou certificats numériques.

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/

GRAND EST CYBERSECURITE

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

+ D'INFO

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

CYBERMALVEILLANCE

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

THÉSÉE

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

L'ANSSI

Renforcer le niveau de cybersécurité
https://cyber.gouv.fr

PERCEV@L

Signaler une utilisation frauduleuse de votre carte bancaire sur internet

PHAROS

Signaler un contenu illicite sur internet
www.internet-signalement.gouv.fr

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

La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Année 2025 – Hors Série n°02

ALERTE AU FAUX COURSIER

Dérivé du Vishing et Spoofing

DIFFUSION LIBRE

Un escroc se fait passer pour le service fraude de votre banque et vous contacte par téléphone pour vous alerter au sujet de transactions suspectes sur votre compte.

Le numéro affiché peut correspondre à celui de votre banque grâce à une technique dite de « spoofing », qui permet d'usurper n'importe quel numéro.

Par le biais d'un vol antérieur de données, le fraudeur dispose déjà de vos informations personnelles (nom, adresse, banque, numéro de carte, etc) renforçant la crédibilité de son discours.

Il adopte un ton rassurant mais se montre pressant, évoquant des débits frauduleux en cours actuellement et prétendant pouvoir les bloquer en temps réel.

Sous couvert d'une prétendue sécurité, il vous annonce qu'un coursier mandaté par la banque va venir récupérer votre carte bancaire afin de la destruire. Parfois, il vous demande d'ailleurs de la couper en deux, sans endommager la puce ou d'indiquer votre code confidentiel. Peu après, un complice se présente à votre domicile et repart avec votre carte.

Celle-ci est ensuite utilisée dans le but de réaliser des retraits ou des paiements frauduleux.

💡 Bon à savoir :

Ne communiquez aucune information bancaire ni personnelle par téléphone. Votre conseiller peut y accéder et n'a pas besoin de vous demander quoi que se soit.

⚠ Ne tombez pas dans le piège !

- ✅ Ne confiez pas votre carte bleue à un inconnu.
- ✅ Au besoin, déposez vous même votre carte à votre banque.
- ✅ Un code d'annulation de transaction n'existe pas.
- ✅ **Ne communiquez jamais vos codes confidentiels**.

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

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.

CYBERMALVEILLANCE

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

THÉSÉE

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

L'ANSSI

Renforcer le niveau de cybersécurité
https://cyber.gouv.fr

PERCEV@L

Signaler une utilisation frauduleuse de votre carte bancaire sur internet

PHAROS

Signaler un contenu illicite sur internet
www.internet-signalement.gouv.fr

+ 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