FICHE REFLEXE CYBERSECURITE

MOBILIANS

Méthodes de Phishing

SIV

Type 1 : se faire passer pour un service de l'Administration

1. Envoi d'un e-mail de type : « *contrôle urgent* », « *suspension habilitation* », *"guide.immat.ants","france securité", "conformité.contrôle","controleur.com", etc*
2. Demande d'appeler au numéro indiqué.
3. Prise de contrôle du poste via un logiciel d'assistance par exemple TeamViewer
4. Demande de brancher la clé SIV et de saisir le PIN.
5. Extraction de la clé privée + identifiants.

Controle de votre habilitation SIV Boîte de réception ×

ANTS <controle@delivrancedestitres-ants.com>
À moi

RÉPUBLIQUE FRANÇAISE
ANTS

Bonjou

Je vous invite a contacter le controleur responsable, en charge d'examiner une partie ou l'ensemble de vos demarche

Il est important de prendre contact avant le **LUNDI 21 JUILLET 2025** afin de permettre aux services de verifier la con

Veuillez repondre a ce courriel en confirmant si vous etes actuellement sous agrement. Le controleur vous fera parve

***Je vous demande de cesser tout enregistrement dans le SIV temporairement en attendant de prendre contac**

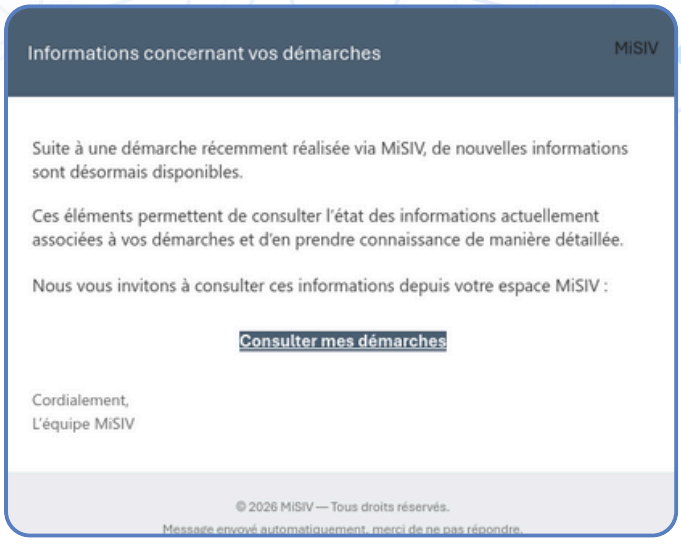
Pour toute question concernant le controle, vous pouvez contacter le numero suivant : 01.59.62.41.00

Je vous rappelle que l'absence de reponse ou la non-execution des demandes mentionnes ci-dessus constituerait un

Cordialement,
ANTS - Expertise et Services
Service Verification
*Tel : **01.59.62.41.00** | Email : controle@delivrancedestitres-ants.com*

Aucun service de l'Etat ne demandera aux professionnels de l'automobile habilités des informations relatives à leur habilitation ou agrément SIV, certificats numériques ou codes secrets.

Type 2 : se faire passer pour un concentrateur SIV



Informations concernant vos démarches MiSIV

Suite à une démarche récemment réalisée via MiSIV, de nouvelles informations sont désormais disponibles.

Ces éléments permettent de consulter l'état des informations actuellement associées à vos démarches et d'en prendre connaissance de manière détaillée.

Nous vous invitons à consulter ces informations depuis votre espace MiSIV :

Consulter mes démarches

Cordialement,
L'équipe MiSIV

© 2026 MiSIV — Tous droits réservés.
Message envoyé automatiquement, merci de ne pas répondre.

Les attaquants se font passer pour l'éditeur de logiciel avec un message parfois très simple vous invitant à consulter une information sur le portail. Vous saisissez votre identifiant et mot de passe via une fausse page de login. Vos identifiants, aussi complexes soient-ils sont instantanément dérobés.

Veillez à toujours utiliser la bonne page web

MOBILIANS

ANTICIPER
REAGIR
ALERTER

Comment se protéger ?

· **Vérifier** l'adresse e-mail de l'expéditeur du message
· Ne jamais installer de **logiciel d'assistance** à la demande d'un prétendu contrôleur
· Ne jamais communiquer vos identifiants
.Ne jamais enregistrer de mots de passe et veiller à les changer régulièrement
. Regarder régulièrement l'historique des opérations demandées pour d'éventuelles anomalies
· Retirer **systématiquement** la clé SIV à la fin de chaque journée, les piratages ont lieu le soir et les week-ends
· Utiliser une **adresse mail spécifique dédiée aux démarches SIV.**

En cas de suspicion d'attaque :

Débrancher immédiatement la clé SIV,
Changez vos mots de passe.

Et dans le cas où l'attaque a été faite :

1. Alertez immédiatement **votre préfecture** de rattachement pour qu'elle suspende l'habilitation.
2. **Déposez plainte** auprès des autorités compétentes (motif: hameçonnage) (forces de sécurité intérieure ou auprès du Parquet).
3. Signaler sa situation à sa banque pour faire **opposition** au prélèvement à venir.
4. Signaler sa situation au CECI de Toulouse si des opérations payantes ont été effectuées et si le PCA paye par prélèvement automatique : **ceci-toulouse@dgfip.finances.gouv.fr.**
5. Signalez-le immédiatement à l'adresse **siv-pha@interieur.gouv.fr.**
6. Faites une **capture écran** de toutes les prestations d'immatriculations effectuées à votre insu et communiquer toute cela à la préfecture.
7. **Signalez ce mail** comme « phishing ou hameçonnage » auprès des plateformes https://www.signal-spam.fr/Let https://cybermalveillance.gouv.fr/.
8. Demandez l**a révocation du/des certificat(s) compromis** auprès du fournisseur (autorité de certification).
9. Modifiez l'ensemble de vos mots de passe, notamment celui de votre compte Certifié Pro sur le site de France Titres, **créez une adresse mail** de contact exclusivement dédiée aux échanges avec l'administration.
10. **Vérifiez votre compte** professionnel SIV pour vous assurer qu'aucun certificat frauduleux n'y a été rattaché.
11. **Contactez Mobilians**