Notre Temps fait le point

"Info ANTAI/ Vous avez un retard de paiement de 35€", "Consulter mon dossier d'infraction via ….". Attention si vous recevez ce genre de SMS! Ce type de message pullule sur nos téléphones et nos courriels depuis quelques mois. Après les faux colis et l'Assurance maladie, c'est au tour de l'Agence nationale du traitement automatisé des infractions (ANTAI) d'alerter sur ce phénomène. Des **escrocs se font passer pour l'Agence et demandent le règlement d'une amende de stationnement** avec votre numéro de dossier via un lien qui vous est communiqué. Sauf que ce lien, tout comme le message, est frauduleux et vous envoie vers des sites pirates. Le but des cybercriminels: collecter vos informations personnelles et vos coordonnées bancaires. **Ne cliquez surtout pas!** Cette technique, appelée "**Phishing**" (hameçonnage en Français), est en augmentation depuis ces dernières années et touche de plus en plus de sites gouvernementaux. Comment les identifier et les différencier des réels messages? Voici quelques conseils.

L’ANTAI n’envoie jamais de SMS

Si vous recevez un SMS de l'ANTAI vous demandant de régler une amende de stationnement, sachez que c'est une arnaque! L'agence gouvernementale **n'envoie jamais de SMS pour demander vos informations personnelles ou financières. De façon générale, ne communiquez jamais d'informations sensibles** par messagerie, téléphone ou formulaire en ligne: aucune administration ne vous demandera vos données bancaires, vos mots de passe, etc.

L'unique moment où vous pouvez payer votre amende par SMS est lorsque vous vous faites verbaliser par un agent des forces de l'ordre et **qu'il vous envoie en sa présence** un QR code pour le règlement de la contravention.
Le lien de paiement reçu doit pointer directement vers le site officiel www.amendes.gouv.fr

Lorsque l'agence nationale veut vous contacter, cela s'effectue que **par courrier.** Si toutefois vous recevez un mail provenant de leur part, assurez-vous de son authenticité. Ceux de l'ANTAI sont uniquement sous l'adresse ***nepasrepondre_noreply@antai.fr*.**

SMS douteux? Vérifiez l’URL du lien

Retenez bien que pour tous les sites du gouvernement, **les liens envoyés finissent toujours par "*.gouv*"**. Ceux qui sont frauduleux se terminent généralement par "*.app*". Pour vous aider, voici la liste des sites officiels:

- **Paiement des amendes:** *www.amendes.gouv.fr*
- **Paiement du stationnement**: *www.stationnement.gouv.fr*
- **Le site officiel de l'ANTAI, qui permet la consultation ou contestation des amendes est** www.antai.gouv.fr

Fausse amende: comment reconnaitre un site frauduleux?

Sur la plateforme officielle de règlement des amendes routières, vous êtes invité à **scanner un QR code ou votre numéro d'infraction reçu sur l'avis de contraventions par courrier.** Sur ces sites frauduleux, on vous demande simplement de remplir un formulaire dans lequel vous mettez votre nom, prénom, date de naissance et code postal. Ensuite, vous êtes redirigé vers votre amende (généralement de 35€) à payer pour défaut de stationnement, mais **sans la date et le lieu de l'infraction. Méfiance…** Puis, lorsque vous vous apprêtez à la régler, le site renvoie vers une fausse interface de paiement sauf qu'en réalité il s'agit d'un formulaire qui va enregistrer toutes vos informations et coordonnées bancaires dans un fichier.

Que faire en cas d'hameçonnage?

Trop tard, vous avez rempli le fichier frauduleux ou cliquez sur le lien? **Faites immédiatement opposition à votre carte**. Vos données bancaires pourraient être utilisées par des escrocs experts en cybercriminalités. Vous pouvez ensuite signaler votre escroquerie auprès du site officiel du ministère de l'Intérieur Pharos.

Ces sites frauduleux restent en ligne quelques jours, le temps d'hameçonner quelques personnes, avant d'être supprimés par des signalements. Mais généralement, lorsqu'un site ferme, c'en est un autre qui émerge. N'hésitez pas en parler à vos proches et à les mettre en garde.