Escroqueries

Nouvelles arnaques par SMS : les reconnaître et les éviter !

Publié le 09 février 2023 - Direction de l'information légale et administrative (Premier ministre)
Crédits : fizkes - stock.adobe.com

Retard de paiement d'une amende, indemnité carburant, vignette Crit’air... Depuis quelques temps, les arnaques par SMS se multiplient et sont de plus en plus difficiles à identifier. Ces multiples tentatives d’escroqueries n’ont qu’un seul but : récupérer vos données personnelles et bancaires. *Service-Public.fr* vous présente les plus récentes et vous conseille pour vous aider à les repérer et les éviter.

Comme beaucoup de Français, il est probable que vous ayez reçu un de ces SMS provenant de cybercriminels. Le procédé est souvent le même, que ce soit un colis à récupérer ou un mot de passe à changer. Leur objectif est de vous amener à cliquer sur un lien qui récupérera vos données personnelles. Désormais, les escrocs se font aussi passer pour des sites administratifs et usurpent l'identité de certains services publics.

Retard de paiement d'une amende

Dans une arnaque récente, les escrocs se font passer pour l’Agence nationale de traitement automatisé des infractions (Antai). Des SMS frauduleux mentionnent un retard de paiement pour une amende et essaient de récupérer vos informations personnelles ou vos données bancaires. Le principe est simple, le SMS prétexte que le destinataire a un « retard de paiement d'une amende », le message est suivi d’un lien amenant vers un site frauduleux comme « amende-gouv.org », « dossier-antai-gouv.info », etc. Attention ! Si vous cliquez sur ce lien, vous pouvez transmettre vos informations personnelles.

L'Antai rappelle que tout SMS ne peut être transmis qu’en présence d’un agent des forces de l’ordre et qu’il n'existe qu’un seul site pour régler ses contraventions : amendes.gouv.fr.

Un SMS de verbalisation pour un paiement immédiat reçu sans la présence d'un agent verbalisateur est une arnaque. L'Antai préconise de ne surtout pas cliquer sur le lien.

Indemnité carburant

Une autre arnaque courante est d'envoyer un SMS invitant l'usager à réclamer l'indemnité carburant. L'escroc envoie un message qui suggère de cliquer sur un lien pour réclamer ce coup de pouce de 100 €. En réalité les arnaqueurs usurpent l'identité de la Direction générale des finances publiques (DGFIP). Celle-ci met en garde les usagers et affirme que le seul moyen d'obtenir cette aide est de se rendre sur le site impots.gouv.fr, de remplir le formulaire soi-même en entrant son numéro fiscal et celui de sa plaque d'immatriculation et de certifier par une « déclaration sur l'honneur » que vous devez utiliser votre voiture pour vous rendre sur votre lieu de travail. Pour en savoir plus, consultez l'article d'actualité « Indemnité carburant 2023 : 100 euros pour les travailleurs modestes ».

La DGFIP n'envoie jamais de SMS pour faire la promotion de l'indemnité carburant.

Vignette Crit'air

Le ministère de la Transition écologique et de la Cohésion des territoires préconise également la vigilance, en particulier pour les vignettes Crit'air.

Le certificat qualité de l'air Crit'air est une vignette à coller sur son pare-brise. Il est obligatoire si vous circulez dans des zones à faibles émissions mobilités (ZFE) ou lors d'un pic de pollution en cas de mise en œuvre de la circulation différenciée. Son prix est de 3,72 €. Pour l'obtenir il suffit de se connecter au site unique et officiel : https://www.certificat-air.gouv.fr/.

Le site officiel Crit'Air du ministère n'envoie pas de messages par SMS aux usagers pour acheter des vignettes, le gouvernement, le ministère de la Transition écologique ou la Préfecture non plus, précise la véritable plateforme gouvernementale.

Comment reconnaître une arnaque ?

Les arnaques sont de plus en plus difficiles à repérer : nulle faute d'orthographe, un site très proche du vrai, codes visuels du gouvernement... La seule différence facile à identifier réside dans l'adresse du lien (url), elle n'est pas conforme à celle du véritable site officiel. Ainsi, tout site de ministère ne finissant pas par « *gouv.fr* » doit vous mettre la puce à l'oreille. Vous pouvez également vérifier la mention « *https* » dans l'adresse du site. Avant de réaliser le moindre paiement pour une démarche administrative, vérifiez l'identité du site et ses mentions légales.

Suivez les recommandations de la Commission nationale informatique et liberté (CNIL).

Attention : Aucune administration ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone.

Que faire si vous êtes victime d'une escroquerie en ligne ?

Vous pouvez transférer le message au numéro 33 700, la plateforme de signalement des spams vocaux et SMS.

Signalez les escroqueries auprès du site internet-signalement.gouv.fr, la plateforme de l'Office central de lutte contre la criminalité liée aux technologies de l'Information et de la communication.

Pour s'informer sur les escroqueries ou pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : vous pouvez contacter Info Escroqueries au 0 805 805 817 (appel gratuit depuis la France) du lundi au vendredi de 9h à 18h30.

Rendez-vous sur cybermalveillance.gouv.fr, la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance. Elle procure des informations sur les menaces numériques et les moyens de s'en protéger.

Vous pouvez aussi alerter la Direction générale de la de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) qui sanctionne les manquements ou infractions au droit de la consommation. Vous pouvez également signaler un abus sur SignalConso en sélectionnant la rubrique « Démarches administratives ».

Et aussi

- Escroquerie
- Sites de démarches administratives payants : attention aux arnaques !
- Arnaques et pratiques frauduleuses : un nouveau guide de prévention
- Arnaques au RGPD : que faire pour s'en prémunir et si vous en êtes victime ?
- Compte personnel de formation : appels téléphoniques, SMS, attention aux tentatives d'arnaques

Pour en savoir plus

- Attention aux arnaques !
  Direction générale des finances publiques
- Depuis plusieurs jours, des SMS frauduleux vous proposent de payer vos amendes sur des sites pirates.
  Agence nationale de traitement automatisé des infractions
- Arnaques vignettes Crit'Air : le ministère de la Transition écologique et de la Cohésion des territoires appelle à la vigilance
  Ministère chargé de l'environnement