MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

POLICE
NATIONALE

Direction générale de la police nationale

Direction interdépartementale de la police nationale de Seine-et-Marne

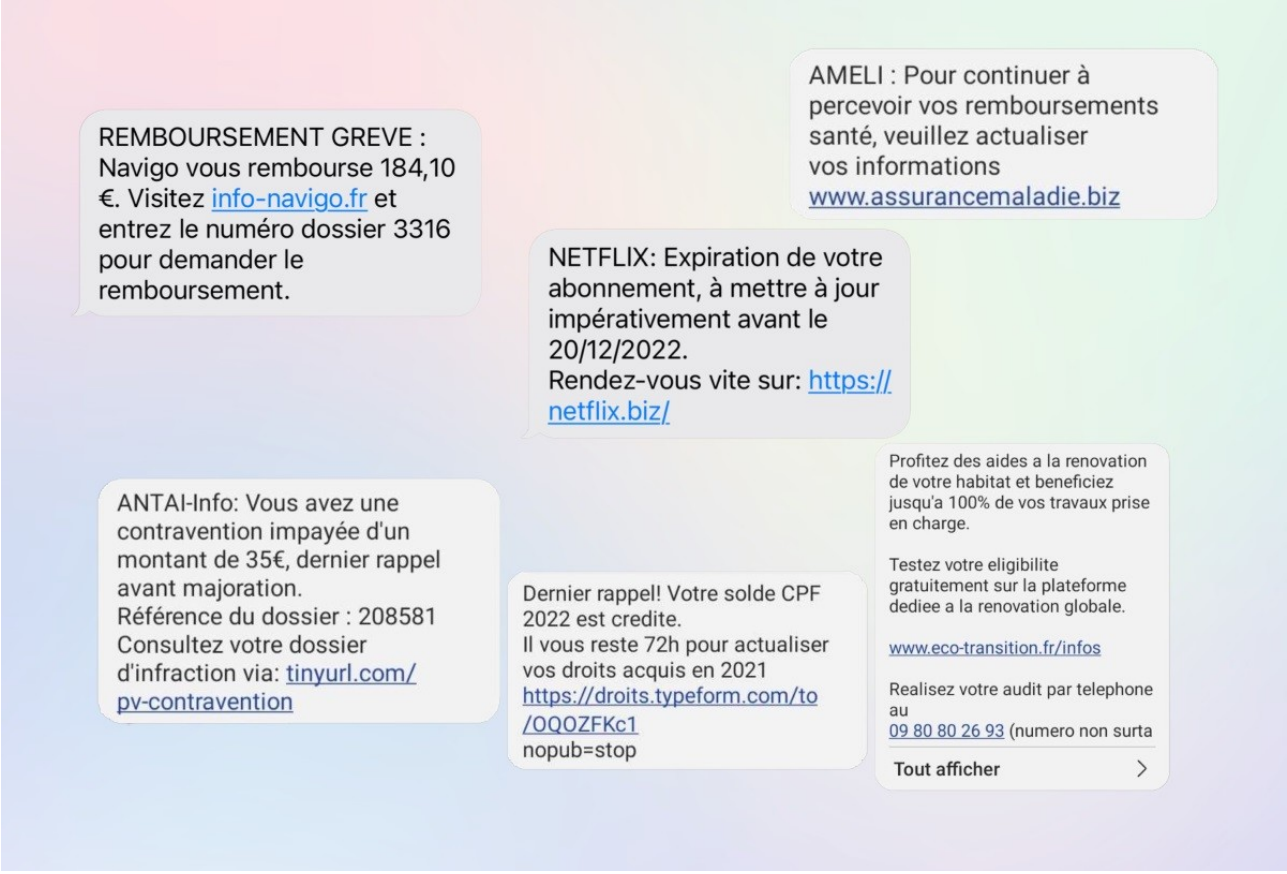
Circonscription de Police Nationale de Melun Val de Seine

La Police Nationale vous informe

Arnaques par SMS:

6 exemples de messages frauduleux

Les arnaques par SMS, appelées «phishing» représentent une menace qui se développe et qui se présente sous différentes formes. Découvrez les types de messages les plus courants:



La plateforme *Cybermalveillance.gouv.fr* précise *que cet hameçonnage par SMS,* offre un avantage aux usurpateurs par rapport aux emails : *«Ils permettent aux cybercriminels de s'exprimer brièvement, avec un langage moins élaboré et plus direct, souvent caractéristique de ce type de*

messages, réduisant ainsi les risques de commettre des fautes d'orthographe ou de syntaxe susceptibles d'éveiller des soupçons.» In fine, le *smishing* peut mener au vol d'informations personnelles, parfois à des fins de revente, ou à l'installation de logiciels malveillants.

Exemples de SMS frauduleux courants

1. Le faux colis

Les messages usurpant les noms de grands services de livraison représentent probablement les cas de *smishing* les plus fréquents. En effet, le SMS étant un mode de communication habituel pour informer de la livraison d'un colis, il est facile pour un pirate de concevoir un faux message renvoyant vers un lien frauduleux. Le message peut prétexter un problème ou simplement proposer de suivre l'acheminement du colis.

2. L'assurance maladie

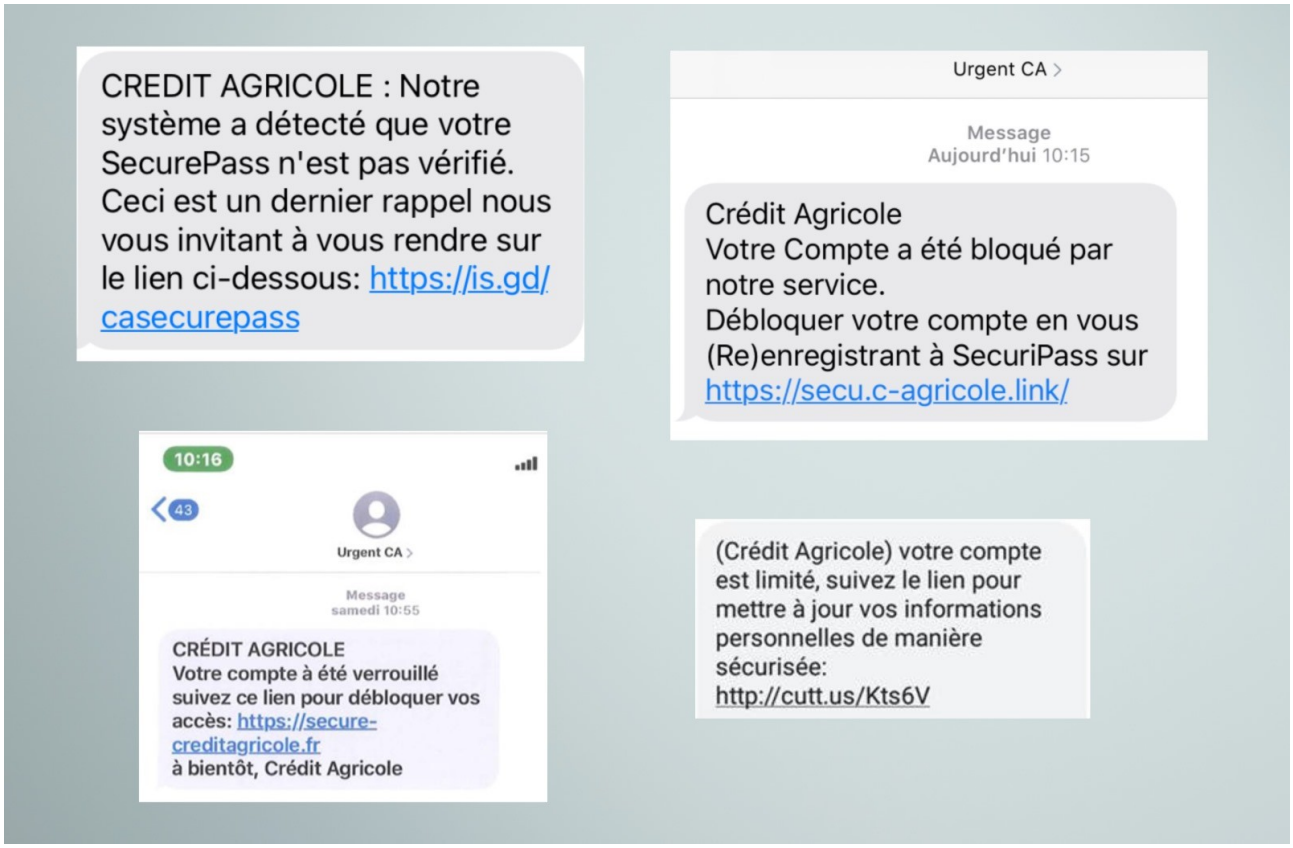
Les faux SMS prétendant venir de l'assurance maladie sont également courants. Sur son espace dédié, ameli met en garde : *«L'Assurance Maladie peut effectivement vous contacter par SMS. Ces messages peuvent inclure des liens vers des pages d'information du site ameli.fr ou votre compte ameli […] Cependant, l'Assurance Maladie ne vous demandera jamais de fournir des informations personnelles (informations médicales, numéro de sécurité sociale, coordonnées bancaires) par SMS.»*

Si vous recevez un message demandant une ou plusieurs informations de cet ordre, il s'agit donc de *smishing*.

3. Les institutions financières

Les messages se faisant passer pour des institutions financières représentent une tactique de *smishing* extrêmement répandue. Les pirates utilisent le nom de grandes banques pour susciter un sentiment d'urgence afin d'inciter l'utilisateur à réagir de manière impulsive. Ces SMS peuvent prétendre que votre compte est verrouillé, qu'un message important doit être consulté, ou qu'un problème est survenu avec le service.

Les banques, de leur côté, alertent régulièrement les utilisateurs sur ces pratiques frauduleuses. Elles rappellent, par exemple, que leurs SMS officiels ne contiennent jamais de liens et qu'aucune information bancaire ne peut être demandée via ce canal.



4. Les amendes ou impôts

Les services de l'État, en tant que figures d'autorité, sont eux aussi ciblés par des usurpations. Bien que cette pratique soit particulièrement courante dans le *phishing* par email, elle est également fréquente pas SMS. Certains services, tels que les Finances Publiques (DGFiP) ou l'Agence Nationale de Traitement Automatisé des Infractions (ANTAI), sont spécifiquement visés par les fraudeurs. Les messages frauduleux prétendent une contravention ou un défaut de paiement, à régler au plus vite.

5. Les vignettes Crit’Air

La vignette Crit’Air est une pastille créée en septembre 2022, qui indique le niveau de pollution des véhicules sur une échelle de 0 à 5. Dans les zones à faibles émissions (ZFE), cette vignette est obligatoire.

Les fraudeurs n’ont pas tardé à se saisir de ce dispositif pour mettre en place des campagnes d’hameçonnage par SMS. Les messages indiquent généralement que vous n’avez pas équipé votre véhicule de cette vignette et vous fournissent un lien pour la télécharger. Dans certains cas, ils mentionnent la possibilité d’une amende en cas de non-téléchargement de la vignette.

6- l'arnaque qui joue sur vos sentiments

“Hello papa, j’ai perdu mon téléphone

Les escrocs en ligne tentent de se faire passer pour vos enfants afin de récupérer de l’argent ou des coordonnées.
“Papa, j’ai perdu mon téléphone c’est mon nouveau numéro enregistre le et envoie-moi un message à ce numéro sur Whatsapp dès que t’as reçu mon message.”
Vous avez peut-être reçu ce message semblant provenir de votre enfant. Le problème, c’est que votre progéniture ne vous a jamais envoyé ce SMS.
Il s’agit en fait d’une arnaque bien rodée, particulièrement efficace et de plus en plus fréquente. Ce message vise à faire croire aux parents que le téléphone de leur enfant est cassé, volé ou perdu et qu’il va avoir besoin d’aide, et surtout d’argent, pour s’en procurer un nouveau. Comme souvent, elle joue sur le sentiment d’urgence via un message alarmant. Une fois le numéro communiqué enregistré sur WhatsApp, le piège se referme. On vous explique.

Il s’agit d’une tentative d’hameçonnage classique…Comment fonctionne le piège ? Dans son SMS, l’escroc va tenter de vous convaincre d’enregistrer son numéro sur WhatsApp.Une fois arrivé sur la messagerie de Meta, les ennuis commencent. Les pirates vous demanderont sûrement de cliquer sur un lien, prétextant souhaiter recevoir de l’argent pour remplacer le téléphone perdu/volé/cassé. Comme dans une tentative d’hameçonnage classique,le but des escrocs est de vous soutirer de l’argent, des informations personnelles ou les deux. C’est en cliquant sur ce lien que vous risquez d’installer par mégarde un logiciel malveillant sur votre téléphone.

Globalement, si les arnaqueurs essaient de vous faire passer par WhatsApp, c’est parce que la messagerie de Meta leur permet plus de facilité en termes de gestion (vous comprenez, gérer plusieurs arnaques en même temps, c’est compliqué). Ce n’est pas pour rien que les arnaques sur WhatsApp sont si nombreuses.

CONSEILS:

- *Ne répondez pas, ne cliquez pas mais transférez à la plateforme de lutte contre les spams vocaux et SMS au 33700*

Votre signalement permettra que d’autres personnes ne se fassent pas arnaquer par le même SMS que celui que vous avez reçu.

Plus il y a de signalements effectués, plus le service est efficace. Les numéros ayant reçu suffisamment de signalements et certifiés frauduleux, seront immédiatement identifiés comme des “spams” auprès des prochains utilisateurs.

Lorsque ce numéro les contactera, une mention “spam ou arnaque possible” sera faite pour les prévenir. Ces numéros associés à des arnaques pourront aussi tout simplement être supprimés par l’opérateur. Donc n’hésitez pas à signaler les SMS suspects !

Souvenez-vous que les escrocs savent coller à l’actualité dans l’unique but de mieux vous dépouiller de vos biens, de vos données personnelles

Comment se protéger du smishing ?

Si les exemples mentionnés précédemment figurent parmi les plus courants, le smishing peut également usurper d’autres types de services (Netflix, Navigo, CPF, etc.) et évolue constamment. Il est donc crucial d’apprendre à identifier les caractéristiques du phishing. Pour vous protéger de l’hameçonnage par SMS, restez vigilants face aux messages reçus, en particulier ceux qui créent un sentiment d’urgence.

Pour reconnaître les SMS frauduleux, Cybermalveillance.gouv offre les cinq conseils suivants :

1. **Ne pas communiquer d’informations sensibles :** les usurpateurs utilisent parfois le nom d’institutions pour demander directement des données personnelles (coordonnées bancaires, mots de passe, etc.). Il est essentiel de ne jamais les fournir par SMS.
2. **Vérifier les informations :** une simple recherche peut souvent révéler si l’information dans le message est authentique. Par exemple, vous pouvez visiter le site officiel de l’organisme mentionné.
3. **Inspecter le lien :** avant de cliquer sur un lien, *« vérifiez sa vraisemblance »*, conseille Cybermalveillance.gouv. La méthode la plus sûre est de rechercher le site par vous-même pour comparer les URL.
4. **Ne pas télécharger d’applications depuis les liens :** les applications doivent être téléchargées uniquement depuis des plateformes fiables telles que l’App Store, le Google Play Store ou le Galaxy Store.
5. **Bloquer l’émetteur :** si vous identifiez un message comme frauduleux, transférez-le par SMS au 33700 pour bloquer son émetteur.

****

Source: BDM Le média des pro du digital
Police Nationale