ASSURÉ

# Attention aux appels, courriels et SMS frauduleux

01 février 2024

L’Assurance Maladie met en garde les assurés sociaux contre des appels téléphoniques frauduleux et contre l'envoi de courriels et de SMS frauduleux. Soyez vigilant ! Comment reconnaître ces sollicitations ? Quels sont les bons réflexes à adopter pour s'en protéger ? L'Assurance Maladie vous donne quelques conseils.

## ATTENTION AUX APPELS TÉLÉPHONIQUES FRAUDULEUX

Des démarchages frauduleux par téléphone qui usurpent le nom de l'Assurance Maladie existent.

Par exemple, lors d'un appel téléphonique se présentant comme provenant de l'Assurance Maladie, l'émetteur de l'appel laissera un message sur votre répondeur vous demandant de rappeler votre CPAM à un numéro différent du 3646. Son but est de vous faire appeler un numéro fortement surtaxé dans le but de vous soutirer de l'argent indirectement. En aucun cas, vous ne devez y donner suite.

Nous vous rappelons que **seul le 3646 (service gratuit + coût de l’appel) vous permet de joindre votre CPAM** et nous vous appelons donc à la vigilance.

Bon à savoir : lorsque l'Assurance Maladie vous contacte par téléphone, le numéro de l'appelant qui s'affiche à l'écran de votre téléphone peut être :

- le 3646 ;
- le 01 78 85 70 03, pour les appels du service sophia ;
- le 01 87 52 00 70, pour les appels menés dans le cadre des opérations Aller vers pour la vaccination contre le Covid-19.

Que ce soit par téléphone ou par mail, l’Assurance Maladie ne vous demandera jamais votre numéro fiscal ou vos identifiants de connexions. Dans certains cas, pour sécuriser les appels, les conseillers de l’Assurance Maladie peuvent demander une partie des coordonnées bancaires (RIB) mais ils ne demanderont jamais la totalité et jamais de mot de passe, même temporaire.

## ATTENTION AUX COURRIELS FRAUDULEUX

L’Assurance Maladie ne demande jamais la communication d’éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par e-mail en dehors de l’espace sécurisé du compte ameli. Tous les messages de ce type en dehors de l’espace du compte ameli sont des tentatives de « phishing », hameçonnage en français.

**Attention, ceci est une escroquerie en ligne, en aucun cas vous ne devez y répondre !**

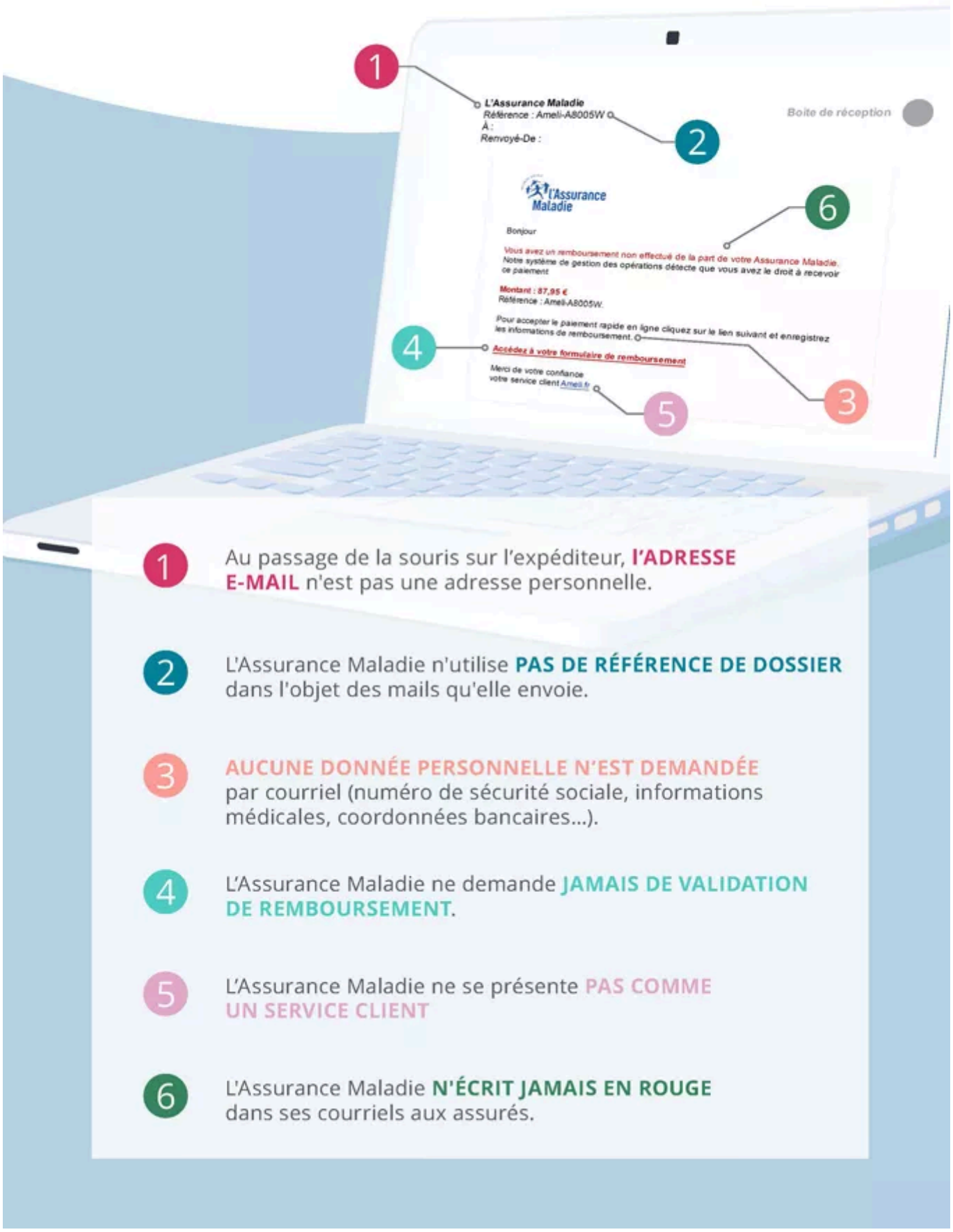
Soyez vigilant ! Cette technique d'escroquerie en ligne est très utilisée. Les escrocs cherchent à obtenir des informations confidentielles afin de s'en servir.

**Vous pouvez aussi vérifier l'expéditeur du courriel**. Quand l’Assurance Maladie adresse un courriel dans la messagerie personnelle d’un assuré et non dans la messagerie de son compte ameli, l’expéditeur qui apparait dans le champ « De » est « Votre Assurance Maladie ». Si l’Assurance Maladie adresse un message d’information ou une newsletter, les adresses mail visibles derrière le nom de l’émetteur sont assurance-maladie@info.ameli.fr ou ne-pas-repondre@app.assurance-maladie.fr. Il est possible de recevoir des courriels concernant Mon espace santé : dans ce cas, l'adresse mail visible derrière le nom de l'émetteur est ne-pas-repondre@monespacesante.fr.

**Pour plus d'informations sur ce piratage et savoir comment vous en protéger :** consultez le site cybermalveillance.gouv.fr.

**Pour signaler un contenu illicite :** connectez-vous sur le portail officiel de signalement de contenus illicites Internet-signalement.gouv.fr.

## Exemple de tentative de hameçonnage




Lire la transcription textuelle de l'infographie

Exemple de tentative de hameçonnage avec le décryptage d'un courriel :

1. Au passage de la souris sur l'expéditeur l'adresse email n'est pas une adresse personnelle.
2. L'Assurance Maladie n'utilise pas de référence de dossier dans l'objet des mails qu'elle envoie.
3. Aucune donnée personnelle n'est demandée par courriel (numéro de sécurité sociale, informations médicales, coordonnées bancaires...).
4. L'Assurance Maladie ne demande jamais de validation de remboursement.
5. L'Assurance Maladie ne se présente pas comme un service client.
6. L'Assurance Madie n'écrit jamais en rouge dans ses courriels aux assurés.

Masquer la transcription textuelle de l'infographie

---

### ATTENTION AUX SMS FRAUDULEUX

L'Assurance Maladie peut vous contacter par SMS. Les SMS de l'Assurance Maladie peuvent contenir des liens vers des pages d'information du site ameli.fr ou vers le compte ameli, auquel vous pouvez accéder en utilisant vos identifiants de connexion.



Mais l'Assurance Maladie ne demande jamais la communication d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par SMS. Tous les messages de ce type sont des tentatives de « smishing » (ou hameçonnage par SMS).

## EXEMPLE DE SMS ET COURRIELS FRAUDULEUX : NOUVELLE CARTE VITALE, REMBOURSEMENT EN ATTENTE DE L'ASSURANCE MALADIE

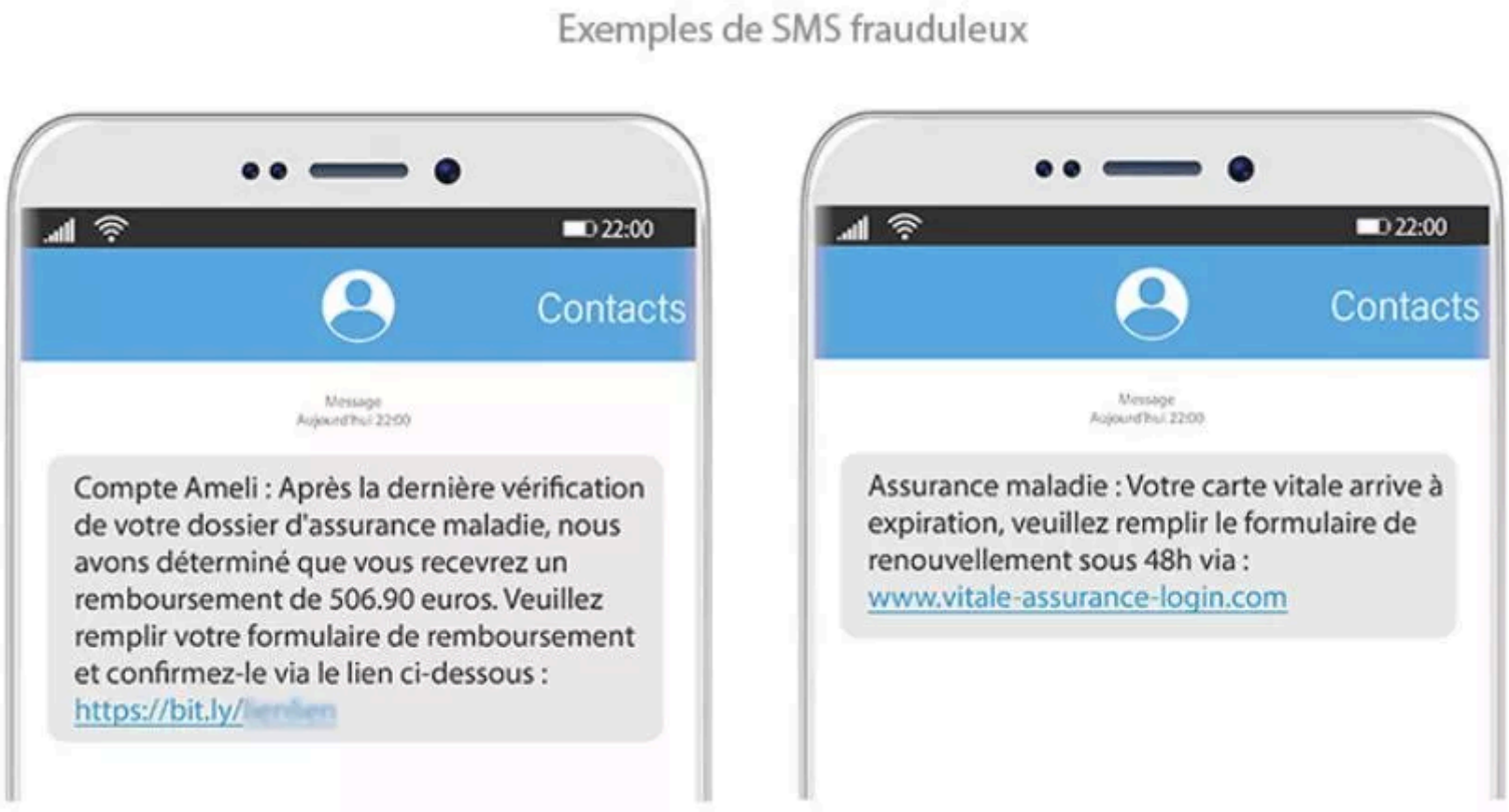
Les fraudes par courriel ou SMS sont nombreuses, elles proposent par exemple :

- un service en ligne payant de mise à jour de la carte Vitale, **alors que la mise à jour de la carte Vitale est totalement gratuite et peut se faire dans la plupart des pharmacies** ;
- le renouvellement de la carte Vitale ou l'arrivée de la carte Vitale 3 ;
- la validation d'un remboursement de l'Assurance Maladie avec un lien cliquable.

Ces messages vous incitent à cliquer sur un lien qui renvoie directement vers un questionnaire visant notamment à recueillir vos coordonnées bancaires ou personnelles.

**Attention, ce sont des escroqueries en ligne, vous ne devez pas y répondre ni cliquer sur le lien !**

Soyez vigilant ! Cette technique d'escroquerie en ligne est très utilisée. Les escrocs cherchent à obtenir des informations confidentielles afin de s'en servir.




## RÉSEAUX SOCIAUX : AUCUNE SOLLICITATION DE L'ASSURANCE MALADIE

Sur les réseaux sociaux, que ce soit en public ou en privé, l'Assurance Maladie n'échange jamais aucune information personnelle (numéro de Sécurité sociale, état de santé…) afin de protéger la vie privée de ses assurés et dans le respect des préconisations de la commission nationale de l'informatique et des libertés (Cnil).

N'hésitez pas à vous abonner au fil X (anciennement Twitter) ou au fil LinkedIn de l'Assurance Maladie : vous y retrouverez toute notre actualité !

## À QUI SIGNALER LES FRAUDES ET LES ARNAQUES ?

Pour signaler un contenu illicite : connectez-vous sur le portail officiel de signalement de contenus illicites Internet-signalement.gouv.fr.

Si vous avez reçu un pourriel (spam), utilisez le site signal-spam.fr.

S'il s'agit d'un SMS, signalez-le sur le site 33700.fr ou en envoyant un SMS au 33 700. Ces services feront bloquer l'émetteur du message.

Agence nationale de la sécurité des systèmes d'information (ANSSI)

internet-signalement.gouv.fr, portail officiel de signalement de contenus illicites de l'Internet

**Cet article vous a-t-il été utile ?**

**OUI** **NON**