Attention aux appels, courriels et SMS

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 (service gratuit + coût de l'appel) ;
- le 01 87 52 00 70, pour les appels menés dans le cadre des opérations Aller vers pour la vaccination contre la Covid-19 ;
- le 09 74 75 76 78, pour les appels menés dans le cadre du dispositif de contact tracing afin de limiter la circulation du virus.

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

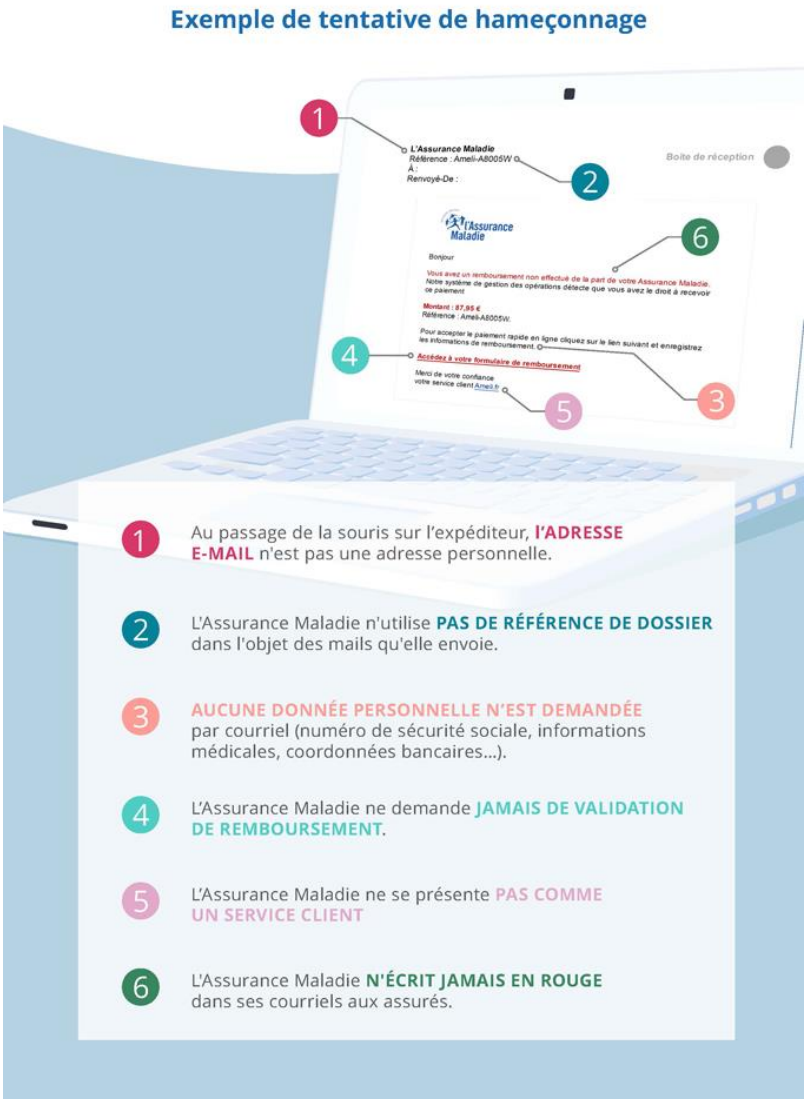
L'Assurance Maladie ne demande jamais la communication d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires) par e-mail en dehors de l'espace sécurisé du compte ameli. Tous les messages de ce type en dehors de l'espace du compte ameli sont des tentatives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

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.



ATTENTION AUX SMS FRAUDULEUX

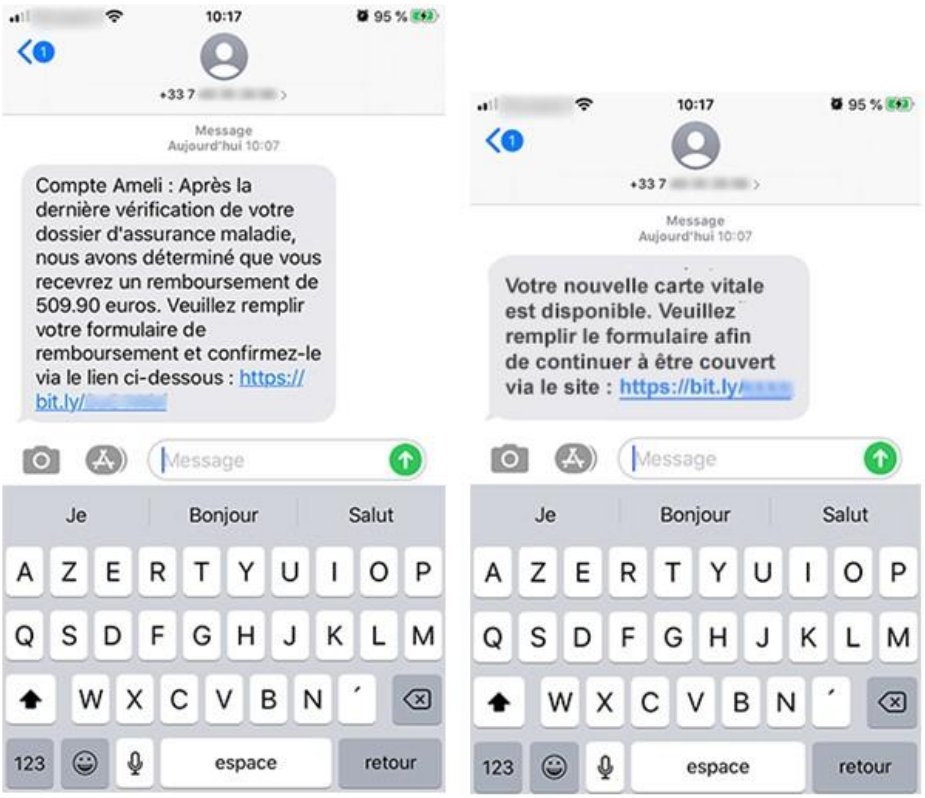
L'Assurance Maladie peut vous contacter par SMS. Les SMS de l'Assurance Maladie peuvent contenir des liens vers des pages d'information du site ameli.fr, ou vers le service declare.ameli.fr ou vers le compte ameli, auquel vous pouvez accéder en utilisant vos identifiants de connexion.

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 frauduleux : nouvelle carte Vitale, remboursement en attente de l'Assurance Maladie

Par exemple, un SMS frauduleux vous est envoyé pour vous signaler la livraison d'une nouvelle carte Vitale. Autre exemple : un SMS frauduleux vous est envoyé pour vous annoncer qu'un remboursement de l'Assurance Maladie est en attente.

Ces SMS 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.

Pendant la crise sanitaire, les fraudes se multiplient

Dans le cadre de la crise sanitaire, l'Assurance Maladie accompagne les personnes qui doivent s'isoler et elle a fait évoluer le contact tracing, son dispositif pour rechercher les chaînes de contamination à la Covid-19. L'Assurance Maladie peut contacter les personnes positives et les personnes cas contact soit par un appel téléphonique soit par SMS. **Ces SMS peuvent prendre la forme de conversation** : les échanges sont guidés et la personne est invitée à répondre par SMS. Ce dispositif pourrait servir de prétexte pour des tentatives de fraudes et l'Assurance Maladie invite à la vigilance. Les SMS de l'Assurance Maladie ne demandent jamais la communication d'éléments personnels (informations médicales, numéro de sécurité sociale ou coordonnées bancaires).

Pour plus d'informations sur ce piratage et savoir comment vous en protéger : consultez les conseils sur 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.

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 Twitter ou au fil LinkedIn de l'Assurance Maladie : vous y retrouverez toute notre actualité !

FranceConnect : attention aux demandes de diffusion d'informations personnelles

FranceConnect est un dispositif d'authentification mis en place par l'État. Il permet de se connecter à son compte ameli grâce à un autre de ses comptes personnels : celui du site impots.gouv.fr ou laposte.fr, par exemple. Inversement : avec les identifiants du compte ameli, il est possible de se connecter à ces comptes personnels. Le dispositif est pratique et sécurisé mais il convient de rester prudent.

L'Assurance Maladie met en garde contre de nombreuses démarches frauduleuses et notamment liées au compte formation. Des démarcheurs proposent des formations financées par le compte formation et demandent des informations personnelles (comme le numéro de sécurité sociale) pour l'inscription. Il est recommandé de ne jamais communiquer d'informations personnelles par téléphone, par SMS ou par courriel. Pour utiliser son compte formation, il existe un seul site officiel à consulter : moncompteformation.gouv.fr.
L'Assurance Maladie appelle à rester attentifs aux tentatives d'escroqueries (sollicitations répétées, parrainages, offres trompeuses).

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.