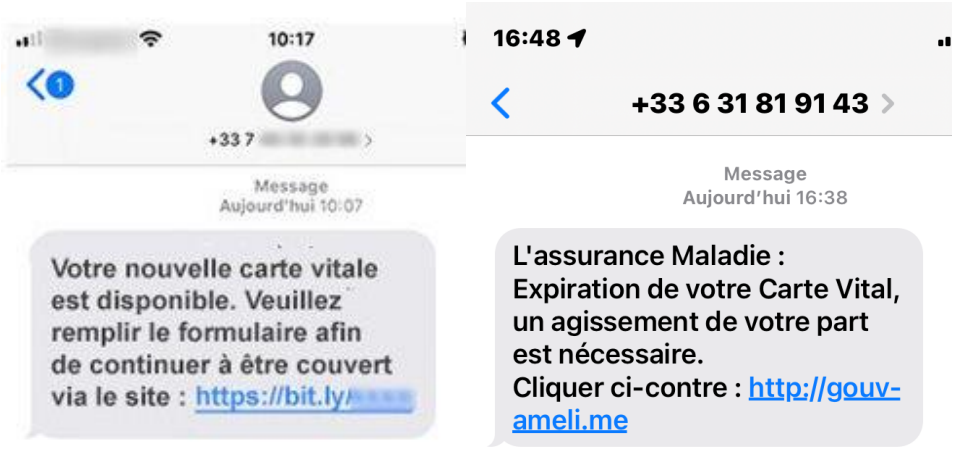
Arnaques au renouvellement de la carte Vitale

L'Assurance Maladie met en garde contre les appels, courriels et SMS frauduleux, de plus en plus fréquents, concernant le renouvellement de carte Vitale. Soyez vigilants face à ce risque !

Cette technique d'escroquerie s'appelle l'hameçonnage (*phishing* en anglais) et concerne tous les internautes. Elle consiste à obtenir de façon illégale des informations personnelles enregistrées sur votre ordinateur (ou tablette numérique ou téléphone).

Si vous fournissez ces données, les auteurs pourront commettre diverses escroqueries, par exemple des fraudes à la carte bancaire, ou des tentatives d'extorsion d'argent.



Exemples de SMS frauduleux : vous recevez sur votre smartphone un message indiquant que votre **nouvelle carte Vitale** est disponible et vous invitant à remplir un formulaire sur un site internet **https://www...**

Ce qu'il faut faire :

- ☞ **ne pas répondre,**
- ☞ **ne pas cliquer sur un texte en surbrillance,**
- ☞ **ne pas l'enregistrer,**
- ☞ **supprimer le message.**

Quelques règles concernant la carte Vitale :

- Elle est gratuite.
- Sa commande, ou son renouvellement s'effectue uniquement avec votre compte « **ameli »,** de même que les déclarations de perte, vol, ou de dysfonctionnement.
- L'Assurance Maladie ne vous demandera jamais la transmission par courriel ou SMS de vos coordonnées bancaires complètes ni de vos informations personnelles.

Les bons gestes si vous avez reçu un message douteux :

- En cas de doute sur un message ou un appel, contactez directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.
- Signaler le message sur les sites spécialisés :
  - https://www.33700.fr/ si vous recevez un SMS ou message vocal frauduleux.
  - https://www.signal-spam.fr/ si vous recevez un courriel frauduleux.

En savoir plus :
Recommandations de l'Assurance Maladie

cernay-info-seniors.fr