

Actuellement, des appels téléphoniques, des courriels et des SMS frauduleux circulent en usurpant l'identité de la caisse d'assurance maladie.

Manière d'opérer

1/ Appels téléphoniques

Vous recevez un appel téléphonique et l'émetteur se présente comme appartenant à l'assurance maladie. La plupart du temps, il vous laisse un message et vous demande de rappeler un numéro surtaxé afin de vous soutirer de l'argent.

Rappel : seul le 3646 permet de joindre la CPAM.

2/ Courriels et SMS

Vous recevez un courriel ou un SMS qui vous invite à remplir un formulaire afin de récupérer votre nouvelle carte vitale ou afin de procéder à un remboursement en votre faveur.

Ceci est une arnaque, un Phishing (hameçonnage), dans le but de récupérer vos données personnelles (informations médicales, numéro de sécurité sociale) et/ou vos coordonnées bancaires.

Rappel : l'Assurance maladie ne vous demandera jamais vos coordonnées bancaires par SMS et ne vous invitera jamais à remplir un formulaire afin de percevoir un remboursement.

Ces échanges se font sur votre compte **Amélie.fr** via un accès sécurisé (identifiant, code personnel).

Conseils

Ne donnez jamais d'informations personnelles par téléphone.

Ne répondez jamais à un courriel ou un SMS vous demandant vos données personnelles ou vos coordonnées bancaires.

Vérifiez toujours l'adresse de l'expéditeur de vos e-mail.

Soyez vigilant, la sûreté est l'affaire de tous.

Retrouvez plus d'informations sur le site de l'assurance maladie en cliquant sur le lien suivant : [Améli.fr](https://www.ameli.fr)