Les SMS, appels ou courriels (e-mails) frauduleux se multiplient.

L'Assurance Maladie met à nouveau en garde les assurés et rappelle qu'il ne faut en aucun cas répondre aux demandes faites par ces messages.

Obtenir une attestation de droits, changer de coordonnées, déclarer une naissance... pour réaliser ces démarches et bien d'autres sans risque et rapidement, c'est facile grâce au compte Ameli ! Pour en savoir plus, consulter la rubrique « Compte Ameli : mode d'emploi ».

Comment les reconnaître pour mieux s'en protéger ?

Ces communications par SMS, appels téléphoniques ou courriels usurpent le nom et le logo de l'Assurance Maladie afin de récupérer des données personnelles ou de faire appeler des numéros surtaxés.

Indices pour repérer les fraudes par téléphone

- Lorsque quelques secondes d'attente s'écoulent entre le moment où l'on décroche et le moment où l'interlocuteur parle, ce temps d'attente peut constituer le 1er indice d'une mise en relation avec une plateforme d'appels frauduleux.
- Le fraudeur tente de rassurer l'assuré et de déjouer sa vigilance en utilisant le nom des services publics officiels ou parfois plus globalement des services de l'État avec lesquels il prétend travailler.
- Le fraudeur dit travailler pour « Ameli » ou pour « l'Assurance Maladie » ou pour le « service digitalisation de FranceConnect en lien avec la Sécurité sociale » ou pour « le compte personnel de formation (CPF) ». Il indique vouloir vérifier le compte Ameli ou le compte FranceConnect ou le compte CPF de l'assuré. Il demande à l'assuré s'il a reçu un courriel (ou e-mail) et comme ce dernier répond non, le fraudeur propose alors de renvoyer le courriel. Il indique ne pouvoir le faire qu'après s'être assuré de la correcte identité de l'assuré et demande l'adresse de messagerie, le numéro de sécurité sociale, le mot de passe du compte ameli, etc. C'est ainsi que les accès au compte ameli de l'assuré sont récupérés par le fraudeur, qui peut alors se rendre sur ce compte ameli pour récupérer les données qui l'intéressent, voire pour modifier des éléments personnels, comme l'adresse mail ou le mot de passe du compte. Le fraudeur peut aussi utiliser les identifiants du compte ameli pour accéder à des sites comme celui du compte personnel formation grâce à l'authentification par FranceConnect.
- Le fraudeur insiste sur le caractère urgent de la démarche à réaliser.

Indices pour repérer les fraudes par courriel (e-mail) ou par SMS

- L'assuré reçoit un courriel qui propose 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).
- L'assuré reçoit un SMS qui signale la livraison d'une nouvelle carte Vitale ou annonce qu'un remboursement de l'Assurance Maladie est en attente avec un lien cliquable.

Face à ces tentatives de fraude, comment se protéger ?

Voici quelques bonnes pratiques à mettre en place pour se protéger de ces fraudes qui sont de plus en plus nombreuses.

Pour effectuer une démarche ou trouver une information, il est important de visiter des sites officiels (comme ameli.fr ou service-public.fr ou les sites du gouvernement dont l'adresse se termine par « .gouv.fr »).

Il est recommandé de vérifier l'expéditeur des courriels avant de les ouvrir ou avant d'effectuer les actions que le message demande de faire.

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.

Attention, les fraudeurs peuvent utiliser des adresses de messagerie très proches avec seulement quelques lettres ou caractères différents.