

FO Arnaque au renouvellement de la carte vitale **Attention à «l'hameçonnage» ou «phishing»** **Energie par SMS ou par mail!**

Des SMS ou courriels vous demandant de renouveler votre carte vitale sont en général destinés à récupérer vos informations bancaires personnelles. Ce phénomène est en hausse continue.

Cela commence par un SMS ou mail... Soyez méfiants et ne communiquez rien!

Vous avez peut-être reçu récemment un message par SMS du type «AMELI : votre carte vitale arrive à expiration...». Attention, vous faites l'objet d'une tentative d'arnaque! Idem pour les mails du même type : ceux de l'Assurance maladie ne comportent jamais de pièce jointe et ne demandent jamais le numéro fiscal ou les identifiants de connexion des assurés.



La carte vitale n'a pas de date d'expiration, il n'y a pas à la renouveler. Elle peut simplement être mise à jour auprès d'un professionnel de santé ou d'une pharmacie sur une borne dédiée



La CAMIEG ne vous demandera aucune information bancaire par téléphone ou lors d'un mail.

Comment se protéger?

Ne jamais cliquer sur un lien contenu dans un SMS ou un courriel pour se rendre sur le site ameli.fr. En cas de doute sur un message, il est toujours préférable de passer par la messagerie de son compte Ameli.

Si vous le pouvez, passez votre souris sur le lien pour l'afficher. Les liens doivent renvoyer vers le site internet ameli.fr ou votre compte ameli (assure.ameli.fr).

Ne jamais communiquer son numéro de sécurité sociale, son numéro fiscal ou ses coordonnées bancaires à un tiers qui n'en a pas l'utilité. Le risque est celui d'une usurpation d'identité.

Comment signaler un problème d'hameçonnage ou de vol de votre numéro de sécurité sociale?

Prévenez au plus vite la CAMIEG. Par internet via votre compte Ameli ou par téléphone au 08 06 06 93 00 (service gratuit + prix d'appel).

Comment signaler une fraude à la carte vitale?

Pour signaler une fraude à la carte vitale, il est possible de procéder à un signalement depuis la plateforme « [PHAROS](#) ».



En cas de courriel frauduleux, le signalement se fait sur le site [signal-spam.fr](#).



S'il s'agit d'un SMS d'hameçonnage, il existe le site [33700.fr](#) pour le signaler ou le numéro 33700 en envoyant un message avec son smartphone.



Que ce soit pour vos données bancaires, fiscales ou de sécurité sociale, la plus grande prudence vous est recommandée. En cas de doute, vous pouvez toujours demander qu'on vous envoie un courrier à votre adresse personnelle, que l'organisme doit forcément avoir.

