Message de remboursement de l'Assurance maladie : attention aux arnaques !

Publié le 18 janvier 2022 - Direction de l'information légale et administrative (Premier ministre)

Illustration 1
Crédits : © peshkov - stock.adobe.com

Vous avez récemment reçu un SMS vous indiquant que vous recevrez un remboursement important de l'Assurance maladie si vous complétez un formulaire ? Vous avez été visé par la nouvelle campagne d'escroquerie circulant sur les téléphones français. Pour ne pas en être victime, *Service-Public.fr* vous rappelle les bons gestes à adopter.

Attention aux arnaques !

L'Assurance maladie a mis à jour ses exemples de SMS, appels et courriels frauduleux. La dernière campagne d'escroquerie vous annonce que vous recevrez un remboursement important après avoir complété un formulaire de remboursement. Soyez vigilant et ne tombez pas dans le piège, c'est une tentative de « *phishing* » ou d'hameçonnage. Cette technique de fraude est aujourd'hui courante sur internet et vise à obtenir des informations personnelles et confidentielles ou à vous escroquer de l'argent.

À savoir : L'Assurance maladie n'est pas la seule entité à connaître ce type d'usurpation d'identité, d'autres organismes comme le Compte Personnel de Formation, la Caisse d'Allocations Familiales ou Pôle-emploi en sont aussi victimes.

Les bons gestes à adopter

Quand vous recevez des messages similaires, il y a trois choses à faire avant de continuer :

1. vérifier l'adresse mail ; en cas de fraude, elle ne dispose pas du nom de domaine de l'entité (ce qui est visible après le @ dans les adresses mail) ;
2. vérifier le numéro de téléphone ; le numéro de téléphone de l'Assurance maladie est le 3646 et en matière de contact tracing du Covid-19, le 0 87 52 00 70 et le 09 86 01 36 46 peuvent vous contacter ;
3. ne pas cliquer sur les liens de ces messages. Connectez-vous sur votre espace personnel, si ce n'est pas une arnaque alors vous y retrouverez les informations communiquées.

De manière générale, les interlocuteurs des entités officielles ne demandent jamais la communication d'informations personnelles ou confidentielles (mot de passe, RIB, numéro de carte bancaire...) hors de votre espace personnel sur leur site. Le contenu du message doit vous interpeller (la promesse d'une importante somme d'argent inattendue) peut vous alerter et vous aider à identifier la tentative de « *phishing* ».

Je suis la cible de ces tentatives d'arnaques, que puis-je faire ?

Vous pouvez signaler la tentative d'arnaque à différents organismes en fonction de sa nature :

- pour signaler un site frauduleux, rendez-vous sur Phishing initiative (https://phishing-initiative.fr/contrib/) ou sur le site du ministère de l'Intérieur (https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action) ;
- pour signaler un courriel ou un site suspect, rendez-vous sur Signal Spam (https://www.signal-spam.fr/) ;
- pour signaler un SMS, rendez-vous sur la plate-forme 33 700 (https://www.33700.fr/) ;
- pour s'informer sur les escroqueries, pour signaler un site internet ou un courriel d'escroqueries, un vol de coordonnées bancaires ou une tentative d'hameçonnage : vous pouvez contacter Info Escroqueries au 0 805 805 817 (appel gratuit depuis la France) du lundi au vendredi de 9h à 18h30.

Je suis victime d'hameçonnage, que faire ?

Si vous avez communiqué vos moyens de paiements, que vous constaté des débits frauduleux, la première étape est de faire opposition immédiatement. Ensuite, en cas d'usurpation d'identité ou de débits frauduleux, conservez les preuves d'hameçonnage, cela vous servira au moment de déposer plainte au commissariat de police ou à la brigade de gendarmerie dont vous dépendez. Et pour finir, il est fondamental de changer vos mots de passe.

Et aussi

- Crédits, livrets d'épargne, assurances : la liste noire des sites douteux s'allonge (https://www.service-public.fr/particuliers/actualites/A15295)
- Compte personnel de formation : appels téléphoniques, SMS, attention aux tentatives d'arnaques (https://www.service-public.fr/particuliers/actualites/A15308)
- Attention aux escroqueries à la livraison de colis ! (https://www.service-public.fr/particuliers/actualites/A15285)

Pour en savoir plus

- Attention aux appels, courriels et SMS frauduleux (https://www.ameli.fr/assure/droits-demarches/principes/attention-appels-courriels-frauduleux)
  Caisse nationale d'assurance maladie (Cnam)