Communiqué de presse

7 avril 2022

#hameçonnage #phishing #arnaque en ligne

L'Assurance Maladie appelle à la prudence face aux tentatives de hameçonnage

Tout au long de l'année de multiples campagnes d'hameçonnage usurpant l'identité de l'Assurance Maladie circulent. Ces messages invitent à compléter un formulaire avec des données personnelles, telles que le numéro de carte bancaire, sous prétexte de recevoir un remboursement de soins ou de régler des frais d'expédition pour l'envoi d'une nouvelle carte Vitale.

Attention ! Il s'agit en réalité d'arnaques dont l'objectif est de dérober des informations personnelles, y compris bancaires, pour en faire un usage frauduleux.

L'Assurance Maladie ne demande jamais la transmission, par email ou SMS, d'éléments personnels (coordonnées bancaires, informations médicales, numéro de sécurité sociale, ou mot de passe). Seuls les échanges d'information via le compte ameli sont sécurisés. Tous les messages de ce type, extérieurs à l'espace du compte ameli, sont des tentatives de « phishing », hameçonnage en français.

Par ailleurs, pour s'assurer qu'un message provient de l'Assurance Maladie, il suffit de vérifier que son adresse expéditrice est assurance-maladie@info.ameli.fr.

En cas de doute sur l'authenticité d'un lien renvoyant vers le compte ameli, il est possible de positionner le curseur de la souris sur le lien, sans cliquer dessus, afin de faire apparaître l'adresse vers laquelle il pointe et vérifier ainsi sa vraisemblance (sur un téléphone, faire un appui long sur le lien). A défaut, il est recommandé de se rendre sur le site de l'Assurance Maladie, ou sur l'application ameli depuis son téléphone mobile ou sa tablette pour se connecter en toute sécurité à son compte.

L'Assurance Maladie a aussi constaté **des appels et messages frauduleux relatifs au nouveau service numérique Mon espace santé** : ceux-ci assurent vouloir « aider à la création de Mon espace santé » en demandant notamment à renseigner les identifiants « France Connect » pour accéder au service numérique. Les risques d'usurpation d'identité sont élevés et peuvent toucher différents services en cas de transmission d'informations (impôts, etc.).

Le numéro fiscal, les identifiants de connexions, etc. pour se connecter aux comptes d'autres administrations, telles que les impôts, ne sont pas demandés par l'Assurance Maladie, que ce soit par téléphone ou par mail. Il est cependant important de savoir que dans certains cas, **pour sécuriser les appels, les conseillers de l'Assurance Maladie peuvent être amenés à demander une partie des chiffres du RIB, mais jamais la totalité, et jamais aucun mot de passe, même temporaire.**

Pour en savoir plus, rendez-vous sur la page dédiée aux usurpations et moyens de s'en prévenir.

A qui signaler les messages frauduleux ?

- **Signalez l'adresse du site d'hameçonnage à** Phishing Initiative qui demandera le blocage de ce site ainsi que sa suppression.
- **S'il s'agit d'un SMS**, signalez-le sur la plateforme 33 700 ou par SMS au 33 700**.** Ces services feront bloquer l'émetteur du message.
- **Si le message frauduleux est** aux couleurs de FranceConnect, il convient de le signaler en le transférant à l'adresse suivante : support.securite@franceconnect.gouv.fr.

Contact presse
presse.cnam@assurance-maladie.fr
Suivez notre actualité sur Twitter !