Données dérobées : l'Assurance Maladie met en garde ses assurés

21 mars 2022

DROITS ET DÉMARCHES

Des personnes non autorisées ont réussi à accéder à des données personnelles administratives concernant environ 500 000 assurés de l'Assurance Maladie d'après les investigations en cours. Elles ont utilisé un service réservé aux professionnels de santé. Il ressort des premières analyses que les attaquants ont pu se connecter à des comptes de professionnels de santé dont les adresses mail avaient été compromises.

Les données concernées sont des données d'identité (nom, prénom, date de naissance, sexe), le numéro de sécurité sociale, ainsi que des données relatives aux droits (déclaration d'un médecin traitant, attribution de la complémentaire santé solidaire ou de l'aide médicale d'État, éventuelle prise en charge à 100 %). Les coordonnées de contact (adresse mail, adresse postale, téléphone), les coordonnées bancaires, ainsi que les données relatives à d'éventuelles maladies ou soins ne sont pas concernées par cet incident.

Chaque assuré concerné va recevoir un courrier ou un courriel de l'Assurance Maladie pour le prévenir et l'alerter sur les risques de hameçonnage/phishing auquel il pourrait être confronté. Le courrier délivrera aussi les consignes de sécurité à respecter ainsi que la démarche à suivre pour signaler tout incident.

L'Assurance Maladie a engagé des poursuites pénales suite à ces agissements et a adressé une notification à la Commission nationale de l'informatique et des libertés (Cnil). Pour garantir la sécurité des accès aux services réservés aux professionnels de santé, l'Assurance Maladie a mis en place des mesures de renforcement de la sécurité sur les comptes amelipro des professionnels de santé.

L'Assurance Maladie tient à rappeler à ses assurés quelques conseils de sécurité à appliquer pour se protéger :

- **pour les messages électroniques reçus** :
  - rester attentif à l'expéditeur des messages, même s'il a l'apparence d'un expéditeur officiel,
  - se méfier des pièces jointes,
  - ne jamais répondre à une demande d'informations confidentielles notamment d'informations bancaires,
  - être attentif au contenu et à la rédaction du message reçu.
- **pour l'accès aux différents services sur internet**, il est recommandé de changer régulièrement les mots de passe de connexion ;
- **pour les appels téléphoniques ou SMS** provenant de numéros inconnus : ne pas répondre aux éventuelles demandes de communication de données personnelles et/ou bancaires.

Pour faire face à d'éventuels arnaques, des ressources en ligne existent :

- l'article « Attention aux appels, courriels et SMS frauduleux » sur ameli ;
- l'article « Les 10 mesures essentielles pour assurer votre cybersécurité » sur le site cybermalveillance.gouv.fr ;

- la rubrique « Les bonnes pratiques » sur le site de l'agence nationale de la sécurité des systèmes d'information ».

Actualité suivante ›

Dernières actualités

› 21/03/2022 - Données dérobées : l'Assurance Maladie met en garde ses assurés

› 18/03/2022 - Covid-19 : comment transformer un ou des certificats sanitaires en un nouveau certificat valide ?

› 17/03/2022 - L'Assurance Maladie active ses dispositifs d'accès aux droits et aux soins auprès des Ukrainiens

› 17/03/2022 - Rémunération des salariés intervenus en renfort pendant la crise sanitaire

› 16/03/2022 - La caisse primaire de Vaucluse organise des conférences sur internet