IMPORTANT

Plusieurs prestataires de tiers payant en France ont été victimes **d'une faille de données**

Le 9 février 2024

Version 001 - 09.02.2024

FAILLE DE DONNEES CHEZ CERTAINS OPERATEURS DE TIERS PAYANT

Vous avez certainement été informé que plusieurs opérateurs de tiers payant en France ont été victimes de plusieurs opérations de vol de données d'une ampleur inédite, et impactant plusieurs acteurs du marché. Ces attaques ont entraîné l'exposition de données à caractèrepersonnel de bénéficiaires.

VIAMEDIS, opérateur de tiers payant sur vos garanties santé, est concerné par cette faille de données.

- Les données personnelles concernées par la faille sont : civilité, nom, prénom, date de naissance, rang de naissance, numéro de sécurité sociale, numéro adhérent, nom du gestionnaire santé.

- Ni informations bancaires, ni données médicales, ni remboursements de santé, ni coordonnées postales, ni numéro de téléphone, ni adresse e-mail, ne sont concernés par cet acte malveillant.

PERSONNES CONCERNEES PAR LA FAILLE

Tous les assurés ne sont pas touchés au regard du mode opératoire de l'attaque sur les opérateurs de tiers payant.

Une information individuelle est réalisée par OCSO à partir du 09 février, via une information disponible sur l'espace santé assuré, puis à compter de la semaine suivante par mail ou courrier.

MES ACCES A MES ESPACES SONT-ILS COMPROMIS ?

Les données concernées ne permettent pas à une personne malveillante d'accéder directement à votre espace assuré ou votre compte AMELI. Sans mot de passe associé, l'accès est impossible.

La fonctionnalité de renouvellement de mots de passe est également sécurisée comme votre accès à vos comptes.

Nous rappelons l'importance d'un mot de passe sécurisé et robuste.

Utilisez des caractères différents : majuscules, minuscules, chiffres, et signes de ponctuation ou caractères spéciaux (€, #...)

N'hésitez pas à renouveler votre mot de passe fréquemment surtout si vous utilisez le même mot de passe sur d'autres plateformes pour vos achats par exemple.

QUE DOIS-JE FAIRE ?

Vous n'avez rien à faire hormis le fait de redoubler de vigilance en cas de sollicitation sous le nom de OCSO.

Les personnes malveillantes ont votre nom, prénom, date de naissance et numéro de sécurité sociale, n° adhérent et connaissent le nom de votre gestionnaire santé.

Il est assez simple pour ces personnes malveillantes de réaliser des campagnes de phishing ou de créer de faux sites internet pour usurper la marque de gestion OCSO.

Nous vous rappelons que par mesure de sécurité, vous ne recevrez jamais de communication ou de sollicitation de notre part vous invitant à saisir ou transmettre des données personnelles ou confidentielles.

OCSO
Groupe DiotSiaci

Les échanges réalisés par les équipes OCSO concernent principalement le suivi administratif de vos dossiers et le traitement des éventuelles réclamations. En cas de doute sur l'origine des messages ou des appels, appelez votre interlocuteur habituel et ayez les bons réflexes en consultant les sites du gouvernement : Hameçonnage ou phishing comment faire ? https://www.economie.gouv.fr

En cas de connexion sur votre espace assuré, restez vigilant à l'URL de connexion : https://www.sante2.ocso.fr

Si vous recevez un e-mail vous invitant à saisir des données personnelles sur un faux site OCSO :

- Ne répondez pas à cet e-mail, il s'agit d'une tentative d'arnaque.
- Supprimez-le de votre messagerie.
- Informez notre service client ou votre interlocuteur habituel.

PUIS-JE UTILISER MA CARTE DE TIERS PAYANT ?

Si vous avez une dépense de santé aujourd'hui ou dans les jours à venir, veuillez noter que :

- Vous pouvez continuer à réaliser vos consultations médicales, soins et présenter votre carte de tiers payant à votre professionnel de santé.
- Concernant les prises en charge en optique, dentaire et audioprothèse, le service peut être perturbé dans les jours à venir.

MESURES PRISES PAR LES OPERATEURS DE TIERS PAYANT ET OCSO

Dès la découverte de cette intrusion, VIAMEDIS a mis en œuvre les actions nécessaires pour isoler et sécuriser la plateforme concernée par cette attaque afin de bloquer les accès non autorisés et en ont informé les autorités.

Le GROUPE DIOT SIACI, propriétaire de la marque de gestion OCSO, a déclenché une cellule de crise pilotée par la Direction Générale pour identifier l'ensemble des mesures nécessaires pour assurer la continuité de services dans un environnement sécurisé.

Nos équipes de cybersécurité sont mobilisées pour accompagner nos clients, les opérateurs de tiers payant et les professionnels de santé faceà cette attaque d'ampleur nationale.

DECLARATION A LA CNIL

Au regard des responsabilités en matière de protection des données personnelles, le groupe DIOT SIACI est co-responsable de traitement avec les assureurs.

En conséquence, le Groupe DIOT SIACI a réalisé une déclaration à la CNIL le vendredi 2 février 2024 sur la base des informations transmises par VIAMEDIS. Les assureurs ont également réalisé des déclarations.

Les entreprises clientes n'ont pas nécessité à réaliser cette déclaration.