IMPORTANT

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

Le 16 février 2024

BIEN-ÊTRE HCR

Version 004 - 16.02.2024

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 caractère personnel de bénéficiaires.

VIAMEDIS ET ALMERYS, opérateurs de tiers payant sur vos garanties santé, sont concernés 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, 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 et les ayants droit sont touchés au regard du mode opératoire de l'attaque sur les opérateurs de tiers payant.

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 HCR.

Les personnes malveillantes ont votre nom, prénom, date de naissance et numéro de sécurité sociale 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 HCR.

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

Dans ce contexte, nous vous invitons à redoubler de vigilance dans les prochaines semaines concernant toutes communications que vous pourriez recevoir et d'adopter les bonnes pratiques suivantes :

- Pensez à changer régulièrement le mot de passe de vos espaces clients et boîtes mails
- Ne transmettez jamais votre identifiant et votre mot de passe par email, SMS ou par téléphone

- Vérifiez bien l'identité de l'expéditeur de mails ou de sms avant de cliquer sur une pièce jointe ou un lien
- Ne cliquez pas sur les liens directement fournis dans les communications que vous pourriez recevoir et connectez vous sur les sites web de vos services habituels

Ayez les bons réflexes en consultant les sites du gouvernement : Hameçonnage ou phishing comment faire ? | economie.gouv.fr et Usurpation d'identité, comment s'en protéger ? | economie.gouv.fr

En cas de connexion sur votre espace assuré, restez vigilant à l'URL de connexion : https://assure.hcrbienetre.fr/connexion.html

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

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

A titre personnel, il vous est possible de déposer plainte si vous le souhaitez, en utilisant le formulaire mis à votre disposition sur le site www.cybermalveillance.gouv.fr.

Pour plus d'informations, vous pouvez vous rendre aux adresses ci-dessous :

- la Commission Nationale de l'Informatique et des Libertés – CNIL
- Cybermalveillance.gouv.fr

De plus, un numéro de téléphone dédié, disponible de 8h30 à 18h au 09 71 10 03 08 (numéro non surtaxé et disponible durant 5 semaines à partir du mercredi 14 février), a été mis en place.

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 selon votre opérateur de tiers payant et votre réseau de soins.

MESURES PRISES PAR LES OPERATEURS DE TIERS PAYANT ET HCR

Dès la découverte de cette intrusion, ALMERYS et VIAMEDIS ont 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.

Nos équipes de cybersécurité ont été mobilisées pour s'assurer que les systèmes informatiques de votre gestionnaire n'ont pas été attaqués et que la continuité de service est assurée.