MCA
Mutuelle Complémentaire d'Alsace

La force de la sérénité

⚠️ INFO : Communication Importante – Cyberattaque chez Almerys avec fuite de données avérée le 23 mai 2026

Notre prestataire **Almerys**, qui gère le tiers payant hospitalier pour le compte de la MCA, a subi une cyberattaque d'envergure nationale.

Cette intrusion a entraîné l'exposition de données personnelles **de plus de 15 millions de personnes assurées auprès de centaines d'organismes complémentaires santé**, y compris le nôtre, à travers toute la France.

La Mutuelle est-elle piratée ?

Non. Dès la connaissance de l'incident, nous avons suspendu toute connexion avec les systèmes d'Almerys et renforcé la surveillance de nos propres systèmes d'information. **Aucune compromission de nos systèmes n'a été détectée à ce jour.** Tous les remboursements et services de la MCA sont pleinement maintenus.

🔍 Le point sur vos données personnelles

Pour vous aider à évaluer la situation, voici le détail précis des données concernées et de celles qui restent parfaitement protégées :

🔴 **Données EXPOSÉES**	🟢 **Données NON CONCERNÉES**
* Nom, prénom, date et rang de naissance	* Coordonnées bancaires
* Numéro de sécurité sociale	* Données de santé, remboursements, soins
* Nom de l'assureur santé et numéro de contrat	* Adresse postale et numéro de téléphone
* Dates de début et de fin de couverture	* Adresse mail et mot de passe MCA (Espace en ligne)

🎯 Quels sont les risques et comment s'en protéger ?

1. Risques potentiels encourus

Des personnes malveillantes pourraient utiliser les données exposées pour :

- Des **tentatives de phishing ciblées** (appels ou e-mails frauduleux usurpant l'identité de la MCA, de la CPAM ou d'un autre organisme pour vous soutirer vos mots de passe, RIB, etc.).
- Des **usurpations d'identité** et fraudes administratives.
- Des **arnaques liées à la santé** ou des fraudes aux prestations.

2. Vos réflexes de sécurité au quotidien

- **Vigilance renforcée :** Soyez extrêmement attentifs aux courriels, SMS ou appels inhabituels de la MCA ou de la Sécurité sociale.
- **En cas de message/appel suspect :**
    - Vérifiez l'identité de l'interlocuteur.
    - Ne répondez pas à l'e-mail, **ne cliquez sur aucun lien :** : il peut s'agir d'un e-mail de hameçonnage qui va vous diriger sur une page frauduleuse qui peut contenir un virus, ou vous demander de saisir des identifiants et mots de passe en se faisant passer pour un organisme de confiance.
    - **Ne communiquez pas vos données sensibles** (coordonnées bancaires, mot de passe, etc.) par téléphone.
    - En cas de doute sur l'authenticité d'un message reçu, contactez directement l'organisme concerné par vos propres moyens.
- **Gestion de vos mots de passe :**
    - Si le Numéro de Sécurité Sociale est l'identifiant d'un de vos comptes, **modifiez immédiatement le mot de passe associé**.
    - Changez régulièrement vos mots de passe (y compris votre espace adhérent).
    - **Règle d'or :** Utilisez un mot de passe robuste (minimum 12 caractères, majuscules, minuscules, chiffres, caractères spéciaux). Évitez les mots du dictionnaire, les prénoms, noms de famille, d'enfants ou d'animaux. N'utilisez jamais le même mot de passe pour plusieurs services (messagerie, réseaux sociaux, service bancaire, etc.).
- **Sur votre Espace Ameli (Assurance Maladie) :** connectez-vous sur www.ameli.fr et vérifiez qu'aucun changement de coordonnées ou ouverture de droits anormale n'a été effectué à votre insu. Activez les notifications de votre compte si ce n'est pas déjà fait.

🛠️ Actions menées par votre Mutuelle

Dès que nous avons été informés par Almerys, nous avons déclenché les actions de protection suivantes :

- **Déclarations légales :** Réalisation des notifications obligatoires auprès de la CNIL et de l'ACPR.
- **Action en justice :** Dépôt de plainte auprès des services de gendarmerie.
- **Sécurité interne :** Surveillance considérablement renforcée de l'ensemble de nos systèmes d'information. Plus largement, la protection de vos données étant une priorité permanente pour notre Mutuelle, nous appliquons au quotidien une stratégie globale de sécurité de nos systèmes d'information.

🚨 Que faire en cas de fraude constatée ?

Si vous remarquez une utilisation frauduleuse de vos données ou une usurpation d'identité :

1. **Changez immédiatement** tous vos mots de passe.
2. **Conservez précieusement toutes les preuves**.
3. **Déposez plainte** au commissariat de police, par écrit au procureur de la République du tribunal judiciaire dont vous dépendez, ou directement en ligne sur le site officiel cybermalveillance.gouv.fr.
4. Vous pouvez également adresser une réclamation sur le site de la **CNIL**.

📞 Nous restons à votre entière disposition

Nos équipes sont pleinement mobilisées pour répondre à toutes vos questions et vous accompagner. Vous pouvez nous joindre :

- ✉️ **Par mail :** dpo@mc-alsace.fr
- 📮 **Par courrier :** Mutuelle Complémentaire d'Alsace – 6 route de Rouffach CS40062 – 68027 Colmar Cedex

Soyez assuré(e) que nous suivons la situation avec la plus grande attention aux côtés de notre prestataire Almerys afin de limiter au maximum les impacts de cet incident.

Les équipes de la Mutuelle Complémentaire d'Alsace