Académie de Grenoble

Grenoble le 22/02/2024

CONSEQUENCES DE L'ACTE MALVEILLANT INFORMATIQUE DONT LES OPERATEURS DE TIERS PAYANT ONT ETE LA CIBLE

Les assureurs du régime santé des établissements scolaires privés et la Commission paritaire nationale tiennent à vous éclairer sur les conséquences d'un acte malveillant informatique dont certains Opérateurs de Tiers payant ont été la cible, en particulier Viamedis et Almerys. Ces réseaux assurent la relation entre les professionnels de santé, l'assurance maladie et les complémentaires santé pour dispenser les assurés d'avance de frais.

Sur le régime santé de l'enseignement privé, les opérateurs impactés sont utilisés par Harmonie mutuelle et Aesio mutuelle. CGRM et Génération qui gèrent les contrats d'AG2R, d'Apicil et d'Uniprévoyance ne sont pas concernés à ce jour, au stade actuel des investigations.

Des données personnelles de bénéficiaires ont été exposées, à savoir les nom,-prénom, date de naissance, numéro de Sécurité sociale, nom de l'assureur santé-et numéro de contrat de l'assureur.
Ni les informations bancaires, ni les données de santé, ni les coordonnées postales, ni les numéros de téléphone, ni les adresses email, ne sont concernés par cet acte malveillant.

Pour Harmonie Mutuelle, tous les assurés ne sont pas concernés par le piratage. Ceux qui ont été impactés recevront d'Harmonie Mutuelle un courrier individuel, dans les meilleurs délais.

Pour Aésio Mutuelle, une communication emailing à destination des adhérents a d'ores-et-déjà été envoyée, rappelant les recommandations de vigilance. Une alerte est également disponible sur la page d'accueil du site internet.

Quel que soit son assureur ou son gestionnaire du contrat santé, il est important de faire preuve de vigilance et d'inviter à redoubler de vigilance et à respecter les recommandations disponibles sur le site cybermalveilance.gouv.fr :

- Changer régulièrement le mot de passe sur chacun de ses espaces en ligne (espaces clients, boîte mail, etc...)
- Rester vigilant et ne saisir en aucun cas un mot de passe lorsqu'il y a un doute de fiabilité du site visité
- Ne jamais transmettre son identifiant ou mot de passe par email, SMS ou par téléphone. Les gestionnaires santé ne demandent jamais ces renseignements. Toute demande de cet ordre est donc suspecte.
- Ne pas ouvrir d'email, de pièce jointe ou de lien dont on ne connaitrait pas l'émetteur et dont le contenu semblerait inhabituel.

Nous nous excusons par avance des perturbations éventuelles des services de Tiers-Payant (avance de frais)