Détournement de données personnelles

Par yapasdequoi

Bonjour à tous,

Ma mutuelle m'informe que je fais partie des (nombreuses) victimes d'un récent détournement de données personnelles.

"Cet acte de malveillance a pu avoir pour conséquence l'accès non autorisé à vos données via notre opérateur de Tiers payant. Les données personnelles exposées sont limitées et sont les suivantes pour vous-même et votre famille : nom, prénom, date de naissance, numéro de Sécurité sociale, nom de votre assureur santé, numéro de votre contrat.

Les données bancaires, les données médicales, les remboursements de santé, les coordonnées postales, les numéros de téléphone, les adresses email ne sont pas concernés par cet acte malveillant."

J'ai l'impression que ce message est un peu trop rassurant..

Que risquons-nous réellement ? Y a-t-il des précautions particulières à prendre ?

Merci de vos éclairages.

Par chaber

bonjour

reçu ce midi
""Toujours selon la CNIL, les prestataires Viamedis et Almerys se doivent d'informer individuellement chaque victime. L'organisme de sécurité, quant à lui, veillera à ce que cette information soit transmise dans les plus brefs délais.

Aucune date n'est pour l'instant annoncée pour cette communication de crise auprès des principaux concernés. Néanmoins, selon TF1, vous avez la possibilité de savoir si vos informations personnelles ont déjà été piratées par le passé, en entrant simplement votre adresse mail sur le site ?haveibeenpwned.com?. ""

Par LaChaumerande

Bonjour

Reçu ce matin ce mail, un peu long,

Chère cliente, Cher client,
Almerys, prestataire qui réalise les opérations de remboursements complémentaires de soins de santé, a fait l'objet d'une cyberattaque sur la partie tiers-payant.

Par mesure de précaution, *** a déconnecté ses systèmes informatiques de ceux d'Almerys vendredi 2 février afin de vérifier l'ensemble des systèmes et s'assurer de la bonne remédiation à cette situation. De complètes investigations de sécurité ont été effectuées pendant le week-end des 3 et 4 février. Elles nous ont permis de réouvrir le système dès le lundi 5 février.

Vos données personnelles, et celles de votre famille, peuvent avoir été exposées. Cela concerne l'état civil, la date de naissance et le numéro de sécurité sociale, le numéro de contrat de complémentaire santé et dans certains cas le nom de l'assureur.

Les informations bancaires, les données médicales, les garanties de votre contrat d'assurance santé, les remboursements de soins de santé, les coordonnées postales, les numéros de téléphone et contacts mails ne sont pas

concernés par cet acte cybercriminel, car ils ne sont pas stockés sur la plateforme d'Almerys.

Almerys a déposé plainte auprès du procureur de la République et, nous avons notifié l'incident auprès de la CNIL.

En plus des actions menées par Almerys pour enquêter sur l'impact de l'attaque subie, nous avons étendu notre dispositif de veille cyber à la recherche d'une éventuelle diffusion de ces données.

Nous vous informons que vous êtes susceptibles de recevoir des courriels ou SMS frauduleux, qui pourraient vous paraître réalistes. A ce titre, nous vous invitons à être particulièrement vigilants si vous en receviez (comme un prétendu courriel de votre médecin ou de la Sécurité sociale).

Par mesure de précaution, nous vous invitons à modifier votre code confidentiel sur votre espace client *** et à être vigilants, sur votre boîte mail, à d'éventuelles actions d'hameçonnage visant à obtenir de vous des informations bancaires ou des codes confidentiels.

Pour rappel, vos informations bancaires et codes confidentiels ne doivent jamais être communiqués par mail à un quelconque opérateur. Nous vous conseillons de prendre connaissance des recommandations d'usage sur le site du gouvernement : comment réagir en cas de fuite ou violation de données personnelles ? - Assistance aux victimes de cybermalveillance.

Par ailleurs, si vous constatez que votre identité a pu être usurpée, nous vous invitons à consulter les recommandations de la CNIL «Comment réagir face à une usurpation d'identité ?».

Pour toute demande d'information supplémentaire, vous pouvez contacter : ...

Nous vous prions de nous excuser pour la gêne occasionnée.

Voilà, voilà.

Par yapasdequoi

Merci de partager vos messages.

Sans que ce soit dit explicitement, il est donc à craindre que les hackers aient aussi récupéré nos adresses mail...
Ce n'est pas rassurant.

Par Isadore

Bonjour,

De mon côté, c'est notre entreprise qui a averti les salariés. Notre mutuelle ne semble pas avoir été concernée, mais notre direction de la sécurité informatique nous conseille de prévenir nos proches vulnérables.

A en croire nos experts en sécurité informatique, le principal risque au vu de la nature des données serait leur utilisation pour donner de la crédibilité à des arnaques du type hameçonnage ou "faux conseiller" :
[url=https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage]https://www.economie.gouv.fr/particuliers/phishing-hameconnage-filoutage[/url]

Il faut donc faire tourner les consignes de bases auprès des gens de votre entourage qui connaissent mal ce type d'arnaque : on ne donne pas ses coordonnées bancaires ou d'informations personnelles à quelqu'un vous démarche par téléphone en se prétendant être votre conseiller bancaire, le représentant de la mutuelle...

Même si tous vos comptes ont été vidées, on raccroche le téléphone et on rappelle la banque, la mutuelle ou l'Assurance Maladie à partir du numéro trouvé dans l'annuaire.

Le conseiller de la mutuelle, le banquier ou l'agent de n'importe quel organisme officiel n'a pas besoin d'informations personnelles, il les connaît déjà.

Les gens vulnérables doivent être particulièrement informés que ces escrocs utilisent des techniques pour les faire paniquer (les menacer de lourdes amendes, de bloquer l'ordinateur...).

Les escrocs sont des experts en psychologie, il n'y a pas de honte à se faire avoir. Il ne faut pas laisser la culpabilité empêcher les bons réflexes : faire opposition le plus vite possible, déposer plainte... Si on se rend compte qu'il y a eu

une arnaque, faire opposition sans traîner peut parfois permettre de bloquer le paiement avant qu'il ne soit soumis à la banque. Et dans certains cas la banque peut "rappeler" un virement.

Par yapasdequoi

Il suffirait donc d'être hyper vigilant ? j'ai du mal à y croire.

Par janus2

Bonjour,

Un risque parmi d'autres est l'usurpation d'identité. Avec les renseignements récoltés, une personne peut très bien utiliser votre identité pour, par exemple, obtenir un crédit. Et bien entendu, elle ne remboursera pas les mensualités et c'est vers vous que l'organisme se retournera.

Personnellement, c'est ce qui m'inquiète le plus en général (pas dans le cas présent, ma mutuelle m'ayant averti qu'elle ne travaille pas avec les 2 organismes en question), connaissant des personnes victimes de ce genre d'arnaque qui ont mis des années de procédure à faire reconnaitre l'usurpation d'identité.

Par yapasdequoi

En effet, c'est bien ce qui m'inquiète. J'ai l'impression que les mutuelles victimes minimisent le risque.
Savez-vous s'il y a possibilité de s'associer à une plainte collective dans un tel cas ?

Par yapasdequoi

Bonjour,
Un formulaire de plainte en ligne est mis à disposition des victimes :
[url=https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-viamedis-almerys-formulaire-lettre-plainte-electronique]https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/violation-de-donnees-personnelles-viamedis-almerys-formulaire-lettre-plainte-electronique[/url]