31/10/2024 Adrian de San Isidoro

Actu

Piratage de Free : peut-on attaquer l'opérateur en justice ?

Des millions de données personnelles détenues par l'opérateur ont été dérobées par des pirates. Scandalisés, des clients envisagent de porter plainte.

PhotoPQR/Voix du Nord/Zack Ajili

« Nous vous écrivons afin de vous informer que Free a été victime d'une cyberattaque », a reconnu l'opérateur Internet et mobile dans un mail d'alerte envoyé il y a quelques jours aux abonnés concernés. Nom, prénom, adresses mail et postale, numéro de téléphone ou encore IBAN… autant d'informations personnelles qui ont fuité. En tout, l'auteur du piratage a affirmé sur la Toile avoir dérobé 19,2 millions de données clients.

« Ces données auraient déjà été vendues à un tiers contre la somme de 175 000 $ (161 000 €) selon l'escroc, rapporte Damien Bancal, fondateur du blog Zataz, qui traite de l'actualité de la cybersécurité. *Évidemment, l'exactitude de cette somme, tout comme le nombre de données volées, sont à prendre avec des pincettes. Les propos de malfrats étant rarement fiables ! »*

La responsabilité de Free reste à déterminer

Outrés par le vol de leurs données, certains clients de Free se demandent s'il est possible d'attaquer l'opérateur en justice, pointé du doigt pour négligence grave. *« Est-il possible de déposer plainte contre Free, qui n'a pas réussi à protéger mes données personnelles ? »* s'interroge par exemple l'un de nos lecteurs.

*« Il est toujours possible d'engager une action de groupe à l'encontre de l'opérateur télécom, via **une association de consommateurs agréée***, explique Jean-Jacques Latour, directeur expertise cybersécurité pour Cybermalveillance.gouv.fr, qui assiste entre autres les victimes de hacking. *Mais il n'y a aucune certitude que Free soit condamné : se faire cambrioler ne signifie pas nécessairement qu'on a été négligent ! »*

À LIRE AUSSI >>> SFR piraté, attention au détournement de vos données

Une amende jusqu'à 7 % du chiffre d'affaires

Des réserves partagées par Damien Bancal. *« Pour l'heure, c'est surtout l'opérateur qui a subi un préjudice*, estime-t-il. *L'enquête dira si la responsabilité de la fuite incombe à Free ou non. »* En cas de manquement au Règlement général sur la protection des données (RGPD), l'amende peut être salée : jusqu'à 7 % du chiffre d'affaires !

Récemment, le réseau social LinkedIn a ainsi dû payer 310 millions d'euros pour ne pas avoir indiqué clairement aux utilisateurs, avant de recueillir leur consentement, à quelles fins étaient utilisées leurs données personnelles.

Surveillez vos comptes en banque !

Interrogé sur l'origine de cette fuite, Free n'apporte aucun éclairage. Faille logicielle ? Intermédiaire vérolé dans la chaîne de traitement ? Erreur humaine ou même acte malveillant en interne ? À ce jour, la cause du vol reste inconnue. *« Toutes les mesures nécessaires ont été prises immédiatement pour mettre fin à cette attaque et renforcer la protection de nos systèmes d'information*, veut néanmoins rassurer

l'opérateur dans la réponse qu'il nous a faite. *Si les abonnés constatent un prélèvement inhabituel, ne correspondant à aucune date et aucun montant de facture connue, leur banque a l'obligation de les rembourser. »*

Les détenteurs d'un IBAN volé peuvent en effet activer des abonnements ne nécessitant aucune pièce d'identité. Raison pour laquelle il est recommandé de suivre l'état de ses comptes bancaires. *« Les clients disposent d'un délai de 13 mois pour contester un prélèvement non autorisé »*, rappelle Jean-Jacques Latour. Bloquez-le avec le numéro de mandat, inscrit à côté du libellé qui figure sur votre relevé. Cela empêchera l'entreprise de vous débiter.

À LIRE AUSSI >>> Fraude au faux conseiller bancaire : les banques doivent rembourser !

Un formulaire de plainte bientôt en ligne

Attention également aux SMS et appels suspects. *« Avec la divulgation de numéros de téléphone, des cybercriminels vont certainement passer des appels en endossant le rôle de conseiller bancaire, afin de faire valider des opérations frauduleuses*, prévient Damien Bancal. *À chaque sollicitation de ce genre, raccrochez. »* Ne cliquez pas non plus sur les liens contenus dans les messages provenant d'émetteurs inconnus.

Pour documenter l'ampleur de la fraude, un formulaire de plainte va être mis en ligne sous peu sur le site **Cybermalveillance.gouv.fr**. *« Le remplir permettra aux victimes d'avoir une preuve officielle à présenter à leur banque, si jamais elle rechigne à rembourser en cas d'opération non consentie »*, conclut Jean-Jacques Latour.