Association Loisirs et culture

VOL DE DONNÉES, COMMENT RÉAGIR

Jean Marie Herbaux

Table des matières

Face à une intrusion informatique, on se sent mis à nu dans sa chair. Il est pourtant primordial d'y faire face rapidement.

Fin octobre, l'opérateur Free a été victime d'une attaque informatique qui a entraîné des fuites massives de données. Tout ou partie de ses clients ont vu leurs fichiers privés (noms et prénoms, adresses postales et mails, numéros de téléphone, type d'offre souscrite, référence IBAN pour certains, etc.) aspirés par des pirates du web. Si vous êtes client de Free, sachez que l'entreprise est dans l'obligation de vous informer personnellement de cet état de fait. L'entreprise a mis à disposition un numéro de téléphone gratuit (*0 805 921 100*) pour tout renseignement complémentaire.

VOL D'IBAN.

À la suite de cet événement, il se peut que quelques semaines ou mois plus tard, vous soyez dans le viseur des hackeurs. Ces derniers peuvent tenter de vous hameçonner par le biais de faux mails, usurper votre identité, détourner votre ligne de téléphone mobile, voire essayer de réaliser des prélèvements non autorisés. Face à ces menaces éventuelles, vous ne partez pas désarmé. Vérifiez périodiquement si l'adresse mail utilisée pour vous connecter à Free (ou à tout autre site web sur lequel vous possédez un compte et qui aurait été visé par une attaque informatique) a été corrompue en visitant les sites spécialisés Hackcheck d'Avast https://hackcheck.io/ et Have I Been pwned https://haveibeenpwned.com/

Renseignez celle-ci dans la barre de saisie, cliquez sur le bouton Pwned ? ou Check Now. Si le résultat est positif, supprimez le compte ou bien changez vos identifiants en optant pour un sésame puissant à l'aide du site spécialisé Motdepasse.xyz https://www.motdepasse.xyz/

Si vous constatez par ailleurs que vos données privées ont été utilisées à des fins frauduleuses, ne tardez pas à porter plainte à la gendarmerie ou au commissariat le plus proche. Contactez votre banque, y compris en cas de vol d'IBAN. Sur votre appli bancaire, mettez à jour la liste des bénéficiaires autorisés en supprimant ceux qui n'ont plus lieu d'être. Surveillez les mouvements de votre compte et reportez tout mouvement suspect. Renforcez les défenses autour de votre ordinateur et de votre téléphone en forçant les mises à jour des systèmes d'exploitation et antivirus, et en choisissant des boîtes de messageries dotées de puissants bloqueurs

PENSEZ DOUBLE-AUTHENTIFICATION

La validation en deux étapes vise à valider l'accès à un compte client généralement depuis un second appareil : souvent votre smartphone. Cela amplifie le niveau de sécurité puisque, même si un hackeur est parvenu à récupérer vos identifiants, il ne sera pas en mesure d'accéder à votre compte, car il lui manquera votre téléphone pour autoriser l'accès. Il peut s'agir de l'envoi d'un SMS ou d'une notification à valider, ou encore d'un code à usage unique à renseigner. La méthode est quasi imparable et a fait ses preuves, si bien que la plupart des web marchands, administrations et établissements bancaires l'ont adoptée. Activez-la aussi pour vos comptes.
Procédure pour Edge à cette adresse :
https://support.microsoft.com/fr-fr/account-billing/proc%C3%A9dure-d-utilisation-de-la-v%C3%A9rification-en-deux-%C3%A9tapes-avec-votre-compte-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4