Données accessibles

Par Julianmdz

Bonjour,

Inquiet sur la protection de mes données, j'ai analysé les échanges réseaux qu'avait un site web. A ce moment, je me suis aperçu que celles-ci étaient échangées en clair, via une URL, avec seulement mon numéro d'identification.

Sans protection, il est donc possible, en changeant ce numéro d'identification, de récupérer les infos de n'importe quel membre. Ainsi, n'importe qui peut récupérer les informations de tous les membres, en accédant une simple url.

Après leur avoir signalé, ils confirment qu'il n'y a aucun problème de sécurité et menaces de poursuites juridiques. Je souhaiterai savoir s'il y a illégalité d'accéder une url libre sur leur site ? Et s'il n'ont pas obligation de corriger ?

En effet, je souhaiterai savoir à quel point je suis en tord et ils sont en tord en refusant de rectifier le problème ?

Merci d'avance
Julian

Par Isadore

Bonjour,

Difficile de répondre de manière générale. Cela va notamment dépendre de la nature des données collectées (et notamment de si ce sont des informations personnelles telles que l'adresse électronique ou des données publiques telles que la liste des messages publiés sur forum-juridique.net).

Le RGPD et son ancêtre la Loi informatique et libertés imposent une obligation de sécurité que l'on qualifiera de "raisonnable" à celui qui collecte ou stocke des données personnelles. Voici une page avec des références :
https://www.cnil.fr/fr/garantir-la-securite-des-donnees

Point de vue non juridique, je tombe sur un collègue qui code un truc pareil, il prend un coup de code pénal sur le crâne. Même si c'est sur une page qui affiche les variétés de salades du supermarché du coin. C'est du niveau d'un électricien qui bricole une prise sans couper le courant.

Par Julianmdz

Bonjour,

Merci beaucoup pour votre retour, il s'agit effectivement de données privées : e-mail, adresse postale ainsi qu'une image du mot de passe pouvant par la suite être déchiffrée?

Je suis d'accord pour le coup de code pénal sur la tête, mais il s'agit malheureusement ici d'un organisme international de sport, qui a collecté plus de 200 000 coordonnés dont tous les professionnels ?

De ce fait, ayant eu un retour très négatif de leur part, je souhaite diffuser l'information comme quoi ils mettent à disposition ces données et qu'ils ne comptent pas corriger. Sans dévoiler la liste des contacts ni comment les récupérer.. juste informer les membres. Suis-je dans mon droit pour faire ça ?

Merci encore,
Cordialement,
Julian

Par Isadore

Bonjour,

Ah, si le mot de passe n'est pas stocké en clair, de quoi vous plaignez-vous ?

Plus sérieusement, avant de diffuser une information potentiellement exploitable par des personnes malintentionnées, prévenez la CNIL et fendez-vous d'un courrier recommandé à cette organisation mentionnant les références de la page indiquée ci-dessus. Voici comment signaler à la CNIL :
https://www.cnil.fr/fr/cnil-direct/question/reglement-europeen-quand-faut-il-notifier-une-violation-de-donnees-la-cnil

Honnêtement, un signalement à 200 000 personnes, ça revient à publier publiquement qu'il y a une faille. Si vous êtes le premier à la repérer, inutile d'ameuter les individus malveillants.

EDIT : Pardon, si vous agissez en tant que particulier, vous devez passer par une plainte en ligne :
https://www.cnil.fr/fr/plaintes

Par Julianmdz

Bonjour,

Je trouve que publier nom, prénom, adresse et le mot de passe, même s'il est crypté, la clé n'est pas des plus sécurisée et se casse en quelques jours .. c'est quand même une faute importante.

De plus, alors que je leur ai signalé pour qu'ils corrigent, leur réponse était une menace de poursuites judiciaires..

Je vais donc en effet en référer à la CNIL.

Merci,
Cordialement,
Julian

Par Isadore

Oui, bien sûr que c'est une faute grave, ma première phrase était une boutade. Comme je l'ai dit, celui qui a codé cela mériterait d'être assommé à coup de Code pénal. Il n'a pas dû aller au bout du premier semestre de sa formation d'informaticien !

Quant à refuser de corriger...

Par curiosité, ils vous menaçaient de poursuites pour quelle raison ? Signalement de faille de sécurité ? Entrave à la libre diffusion de données personnelles ?

Par Julianmdz

J'avais un doute, mais je suis rassuré :)

En soit, pour eux, malgré toutes les informations que j'ai donné, le service informatique n'a pas vu de problème de sécurité et de possibilité de recuperation des donnée.. on a pas tous le même service informatique :/

Du coup, il disent que si quelqu'un récupère les données, ce n'est que par une attaque de leurs serveurs, pour le coup répréhensible par la loi.

Je suis vraiment déçu par tant de mauvais fois et ce manque de compétence. Surtout cette idée de faire peur quand je leur ai demandé de corriger sous peine de signaler le problème.. je ne trouve vraiment pas normal pour un tel organisme de ne pas protéger les données de ses membres.

Un combat qui peut paraître idiot.. mais j'en ai marre de tous ces pseudos services qui font payer des comptes membres et ne sont même pas capable de faire les efforts pour protéger tout ça :(

En tout cas, merci beaucoup pour ces retours et je vais leur signaler par courrier en recommandé que je vais déposer une plainte auprès de la cnil :)