DÉCEMBRE 2021 : #11

ACTUALITÉS RGPD

By Tchérylène MAIRET - DPO PRO ARCHIVES SYSTEMES

L'EDITO DU DPO

BÆnn_@nn€e_MMXX2!

Chaque année, un DPO attend les résultats d'un palmarès bien singulier : ni Miss France, ni le Ballon d'Or, ni les personnalités préférées des français mais le TOP 20 des pires mots de passe. Si désinvolte et à la fois si peu inspirée, cette liste pourrait se réduire à un seul mot de passe candidat : P.A.S.S.O.I.R.E. !

Ce classement sidère tout autant qu'il inquiète car si votre mot de passe préféré fait partie de la liste, c'est qu'il est facile à retenir donc facile à découvrir. Il est donc recommandé de changer un mot de passe fragile mais également de prendre en compte les facultés d'une machine de le casser pour en créer un nouveau. La Cnil nous donne quelques *astuces*.

Si vous souhaitez générer votre mot de passe solide, il suffit de le construire à partir d'une phrase, ou **une suite de mots** qui fait sens pour vous. Il est important d'utiliser cette suite de mots. En effet, pour casser un mot de passe, un robot va essayer toutes les combinaisons possibles sur un mot du dictionnaire mais pas sur une suite de mots dont il ne peut deviner le sens qu'il a pour vous.

Ensuite vous appliquerez la règle de la Cnil :

- 12 caractères minimum, 1 majuscule, 1 caractère spécial, 1 nombre, 1 signe de ponctuation
- Exemple : Bonne année 2022 Þ BÆnn_@nn€e_MMXX2!

Vous pouvez tester la solidité de votre mot de passe sur le site de la Cnil : « *Générer un mot de passe solide* ». Et pour se convaincre de l'efficacité de suivre les recommandations de la Cnil pour définir un mot de passe solide, Statista [portail en ligne de statistiques] a publié le 1er décembre 2021 *une infographie* sur la robustesse aux attaques : « ***Un mot de passe de douze caractères avec une lettre majuscule, un chiffre et un symbole est presque incassable, il faut 34 000 ans à un ordinateur pour le déchiffrer*** ».

Donc, la vulnérabilité présumée d'un mot de passe n'est pas une fatalité. Enfin, autant de créativité suppose la discrétion. Or il peut être difficile de mémoriser tous ses mots de passe compliqués.

C'est pourquoi, votre DPO vous conseille de sauvegarder tous vos mots de passe de vos sites préférés dans un coffre-fort certifié de l'ANSSI. Votre DPO utilise *Keepass*.

Le coffre-fort est enregistré sur votre ordinateur ou votre smartphone.

- 1 seul mot de passe solide à mémoriser,
- = accès à tous vos mots de passe sauvegardés.

EN BREF

Top 20 des mots de passe les plus utilisés en 2021

Prédictions 2022 : Cinq menaces qui auront un impact sur vos données personnelles et votre vie privée

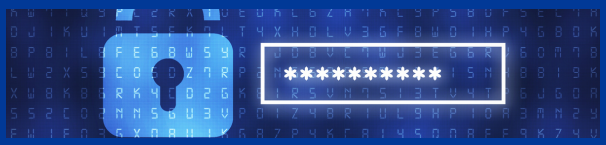
La Cnil donne le feu vert à VIGINUM

QUIC révolutionne le transport des données sur Internet

La Cnil met en demeure Clearview AI de cesser sa collecte biométrique sur Internet

Les données personnelles peuvent être librement transférées entre la Corée du sud et l'Europe

Votre DPO et
PRO ARCHIVES SYSTEMES
vous souhaitent de bonnes fêtes
et une excellente
année 2022
qui vous trouvera, nous
l'espérons, dans les meilleures
dispositions possibles relatives
à la Conformité au RGPD.



TOP 20 DES MOTS DE PASSE LES PLUS UTILISÉS EN 2021

« Doudou » tient la corde avec « 123456 ». Voici les 200 mots de passe les plus courants selon les recherches menées en 2021. Ce classement est établi par pays.

La note du DPO

En 2017, le TOP 20 a vu l'entrée de « Star Wars » des pires mots de passe à l'occasion des 40 ans de la saga de George Lucas. En effet, nous serions sensibles aux termes courants de la culture populaire et du sport.

Voir le top 20

LA CNIL DONNE LE FEU VERT À VIGINUM

Par *décret* n° 2021-1587 du 7 décembre 2021, le Conseil d'Etat donne son feu vert à la collecte de données personnelles extraites en ligne et sur les réseaux sociaux afin de lutter contre la diffusion de fausses nouvelles et l'ingérence de puissances étrangères. C'est le Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM).
Les données collectées ne pourront être conservées que pour une durée maximum de six mois, et les collectes ne pourront être ni « automatiques » ni « constantes », mais déclenchées uniquement après une détection suspecte d'un agent.
Le déploiement de VIGINUM a été autorisé après avis de la Cnil par *délibération* n° 2021-116 du 7 octobre 2021.

En savoir +

LA CNIL MET EN DEMEURE CLEARVIEW AI DE CESSER SA COLLECTE BIOMÉTRIQUE SUR INTERNET

La société américaine est accusée par la Cnil d'avoir développé un logiciel de reconnaissance faciale dont la base de données repose sur l'aspiration de photographies et de vidéos publiquement accessibles sur Internet. La Présidente de la Cnil laisse 2 mois à Clearview AI pour supprimer les données concernées.

La note du DPO

La collecte de ces données biométriques s'effectuant sans base légale, c'est un manquement à l'article 6 du RGPD.

Lire l'article

LES DONNÉES PERSONNELLES PEUVENT ÊTRE LIBREMENT TRANSFÉRÉES ENTRE LA CORÉE DU SUD ET L'EUROPE

La commission européenne a rendu sa décision sur la protection adéquate des données à caractère personnel par la République de Corée le 17 décembre 2021. Les données personnelles peuvent désormais librement circuler des deux côtés sans restriction.

La note du DPO

Rappelons que les USA ont perdu ce privilège d'adéquation avec l'invalidation du Privacy Shield.
Voici la liste des pays dont l'Europe reconnait le même niveau de protection des données personnelles que la réglementation RGPD : Israël, Andorre, Argentine, Japon, Iles Féroé, Guernesey, Ile de Man, Nouvelle Zélande, Suisse, Uruguay, Royaume Uni (période probatoire) et la Corée du Sud.
Néanmoins, les personnes concernées doivent obligatoirement être informées de tout transfert de données personnelles en dehors de l'Union Européenne.

Lire l'article

PRÉDICTIONS 2022 : CINQ MENACES QUI AURONT UN IMPACT SUR VOS DONNÉES PERSONNELLES ET VOTRE VIE PRIVÉE

Le site *Global Security Mag* fait le point pour nous. L'auteur de cet article s'attarde sur 5 cybermenaces majeures :

1. Il sera de plus en plus difficile de distinguer ce qui est légitime en ligne :

«Lors du premier trimestre 2021, 4 personnes sur 10 ont rencontré un lien dangereux en utilisant leurs appareils mobiles. Moins d'un an plus tard, 5 personnes sur 10 ont été confrontées à des menaces au troisième trimestre 2021. Cette tendance ne fera que s'accentuer avec la multiplication des escroqueries par SMS, e-mail et médias sociaux.»

2. Vos données privées seront exposées, il est donc essentiel de sécuriser vos comptes.
3. Les crypto-monnaies vont se généraliser et les escroqueries aux crypto-monnaies vont suivre.
4. L'essor de l'IoT et des "appareils connectés" suscite des inquiétudes quant au respect de la vie privée en raison des données collectées.
5. Les citoyens veulent plus d'anonymat.

«En résumé, l'année 2022 sera marquée par des risques accrus pour notre sécurité numérique, notre vie privée et nos finances, car nous vivons davantage en ligne. Mais il y a une bonne nouvelle : les internautes peuvent prendre des mesures pour se protéger.

En savoir +

QUIC RÉVOLUTIONNE LE TRANSPORT DES DONNÉES SUR INTERNET

[Via *Afnic.fr* Internet Made in France]

Le 27 mai 2021, les normes techniques du protocole de transport Internet QUIC ont été publiées. QUIC pourrait à terme remplacer une grande partie des usages de l'ancien protocole TCP/IP, notamment sur le Web.
TCP/IP est un chef d'œuvre d'ingénierie qui, depuis quarante ans, a fait circuler des quantités colossales de données dans l'Internet, et tourne sur toutes les machines, de l'ordiphone bas de gamme au très gros serveur. Mais les évolutions de l'Internet ont montré des limites à TCP/IP, au moins pour certains usages. D'où le développement, ces dernières années, du protocole QUIC. Celui-ci est désormais normalisé, dans quatre documents, les RFC (Request for Comments) *8999*, *9000*, 9001 et *9002*.
Les avantages :

- QUIC fusionne le transport et le chiffrement,
- QUIC augmente le parallélisme de la communication,
- QUIC permet le changement d'adresse IP en pleine session.

La note du DPO

QUIC permet d'éviter toute attaque-dite de l'Homme du Milieu qui remplace la clé privée du destinataire par la sienne.

En savoir +