Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

POWERiti, l'allié avignonnais des entreprises contre la cybercriminalité

« Protégez-vous contre la cybercriminalité », implore Jantien Rault, le créateur de POWERiti à Avignon, qui se veut une société proposant des solutions informatiques innovantes et sécurisées afin de propulser les entreprises vers une efficacité et une croissance durables.

« 54% des entreprises françaises sont victimes de hackers et ce chiffre explose à une vitesse exponentielle », déclare le créateur de cette start-up qui est le 1er site en France à proposer une offre globale de sécurisation de vos données sensibles.

Lors d'une soirée à l'Hostellerie des Fines Roches de Châteauneuf-du-Pape, ce jeune avignonnais, qui a fait ses études d'informatique et de commerce à Saint-Jean-Baptiste de la Salle et Saint Vincent-Paul, s'est adressé à un parterre d'environ 300 chefs d'entreprises pour les sensibiliser aux risques qu'on entre comme dans un moulin dans leurs mails, fichiers clients, fournisseurs, fiches de paie des salariés,

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

dossiers sensibles stratégiques. « Nous avons '*My serenity*' , une solution tout-en-un (99,90€ par mois) pour rendre impénétrables toutes vos données avec une mise à jour automatique et un support illimité, 100% transparent et sans surprise. »

La cybercriminalité mise en pratique pour cibler les problèmes

Pour faire une démonstration aux chefs d'entreprises, Jeremy Nedjar, venu de la Direction des Finances Publiques, s'est présenté comme 'hacker éthique' de sa société L-Exploit Cyber Expert. « Quand je travaille pour un client, je deviens testeur d'intrusion. Je vois s'il est facile de craquer son mot de passe et c'est souvent le cas. Je me fais passer pour un livreur et j'arrive avec une simple clé USB à entrer dans le réseau et capter toutes les données », martèle-t-il. « On a vu des hôpitaux attaqués pour les données de leurs patients, leur numéro de Sécurité sociale, mais aussi des banques. HSBC, par exemple, a ainsi perdu 1,2Md€, même si on n'a pas tous les chiffres de ce que représente le vol de données. »

> « Il vaut mieux payer une prime pour se protéger qu'une rançon hors de prix d'un hacker malveillant. »
>
> *Jeremy Nedjar*

Il poursuit : « Votre adresse IP, c'est une identification unique, comme votre empreinte digitale. Avant tout, trouvez un code compliqué avec des chiffres, étoiles, slashes, underscores, caractères bizarres, alternez lettres minuscules et majuscules, mais surtout pas toto 1, 2, 3… Sinon, c'est la porte ouverte au sabotage industriel et à la concurrence déloyale. Prémunissez-vous contre ces gens qui veulent forcer votre coffre-fort numérique sans pied-de-biche. Payez 1 000 ou 2 000€ pour sécuriser vos données, ce n'est rien par rapport aux risques encourus. Veillez aussi à ce que vos salariés ne jouent pas avec l'ordinateur du bureau et aient le même code que chez eux, sinon votre entreprise sera vulnérable, donc facilement piratée. 1/3 des sociétés cyberattaquées déposent le bilan quelques mois après. Si vous perdez votre comptabilité, vous ne pouvez plus facturer, bonjour les dégâts. »

POWERiti garantit sécurité et tranquillité

Jantien Rault conclura la soirée en insistant sur l'apport des solutions POWERiti qu'il propose avec ses collaborateurs. « Changer de mot de passe régulièrement, avoir une double authentification, un système anti-phishing, être connecté 24h/24 et 7j/7. Un de ses clients acquiesce : « Avant, dans mon entreprise de 45 salariés et 140M€ de chiffre d'affaires, je faisais tout, même changer le toner de la photocopieuse. J'avais un partenaire informatique nul, qui ne venait jamais quand il y avait une urgence, qui m'avait proposé un contrat de 48 mois totalement opaque, bref, qui était un escroc. Puis, j'ai rencontré Jantien Rault, il a audité scrupuleusement poste après poste, fait des préconisations pour la téléphonie, l'informatique, proposé une maintenance chiffrée, il m'a changé la vie. Certes, ça coûte, mais c'est le prix

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

de ma tranquillité et de la sécurité de ma boîte. En particulier, le retour sur investissement a été rapide grâce à ce qu'il m'a permis d'éviter comme chausse-trappe numérique. »

Contact : global@lxploit.com

Réglementations sur la protection des données & cybersécurité

La sécurité des données personnelles est, au-delà d'une obligation légale, un enjeu majeur pour tous les organismes publics et privés, ainsi que pour tous les individus. 80 % des notifications de violations reçues par la CNIL concernent une perte de confidentialité, c'est-à-dire une intrusion par un tiers qui peut prendre connaissance des données, voire les copier. Retrouvez les dernières infos publiée par la Direction de l'information légale et administrative (DILA).

Développement des systèmes d'intelligence artificielle (IA) : les recommandations de la CNIL

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

En mai 2023, la CNIL avait publié un « plan IA » de sécurisation des acteurs et avait annoncé un travail sur l'encadrement juridique des pratiques. Le 8 avril 2024, la CNIL propose une série de sept recommandations pour accompagner les acteurs dans leurs démarches de conformité avec le règlement général sur la protection des données (RGPD). En savoir plus

Élections européennes 2024 : comment protéger les données des électeurs ?
La Commission nationale de l'informatique et des libertés (CNIL) réactive son dispositif de contrôle des opérations de campagne électorale, cette fois-ci à l'occasion des élections européennes du 9 juin 2024. L'Observatoire des élections permet notamment d'assurer le suivi des signalements des mauvaises pratiques. A lire

Protection des données personnelles : les plaintes enregistrées par la CNIL en hausse en 2023
La Commission nationale de l'informatique et des libertés (CNIL) a enregistré un nombre record de plaintes en 2023 (16 433) soit le double par rapport à avant 2018 (8 360 plaintes en 2017). Par ailleurs, les sites web de la CNIL ont cumulé environ 11,8 millions de visites (800 000 visites de plus qu'en 2022). A découvrir ici

RGPD : bilan européen sur le rôle des délégués à la protection des données personnelles
Un rapport du Comité européen de la protection des données identifie les obstacles auxquels sont confrontés les délégués à la protection des données. Or, ces délégués ont un rôle important dans la mise en conformité au règlement général sur la protection des données (RGPD). Lire l'article

Cybermenaces : quels sont les risques pour la sécurité informatique en France ?
Dans son panorama 2023, l'Agence nationale de la sécurité des systèmes d'information (Anssi) fait état d'une menace informatique qui « continue d'augmenter » dans un contexte de tensions géopolitiques et d'évènements internationaux organisés sur le sol français. Lire l'article

Surveillance des salariés : une amende de 32 millions euros pour Amazon
Dans les entrepôts français d'Amazon, l'activité et les pauses de chaque salarié sont enregistrées et minutées. Selon la Commission nationale de l'informatique et des libertés (CNIL), ce système de surveillance de l'activité et des performances des salariés s'avère « excessivement intrusif ». Consulter

Rapport d'activité 2023 de la Commission nationale de l'informatique et des libertés
L'année 2023 a été marquée par une nette augmentation des sollicitations du grand public, avec 16 433 plaintes traitées par la Commission nationale de l'informatique et des libertés (+ 35 % par rapport à 2022). La CNIL a également été destinataire de 20 810 demandes d'exercice des droits indirect via l'ouverture d'un téléservice dédié (+ 217 % en un an). Lire le rapport

La protection des données personnelles à l'ère de l'internet
Quels ont été les principaux changements apportés à la loi « Informatique et libertés » depuis 1978 ? De quelle manière le Règlement général sur la protection des données a-t-il renforcé les pouvoirs de la CNIL ? Quels sont aujourd'hui les nouveaux risques concernant la protection de la vie privée ? A écouter

« Informatique et libertés » : une loi en avance sur son temps !

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

Quels sont dans les années 1970 les principaux problèmes posés par l'avènement de l'informatique concernant la protection des données et des libertés ? Qu'est-ce que le projet SAFARI ? Pourquoi la commission informatique et libertés a-t-elle été créée ? Quelle est la mission de la CNIL ? A écouter

L.G.

Avignon : la CPME 84 organise un petit-déjeuner sur le thème de la cybersécurité

Le mercredi 24 mai, de 8h à 10h30, vous pourrez participer au petit-déjeuner organisé par la CPME 84, en partenariat avec l'opérateur orange, sur le thème « Cybersécurité : comment protéger ses données ? ».

La CPME 84
La CPME 84 est la première organisation patronale du Vaucluse dédiée spécifiquement aux TPE-PME, commerçants, indépendants et professions libérales du département.

Le sujet
Les enjeux, les menaces et les solutions qui seront évoqués tourneront autour de la nécessité de comprendre le contexte actuel dans les entreprises vis-à-vis des cybermenaces. Il s'agira d'apprendre à identifier les cybermenaces récurrentes pour mieux les appréhender et les éviter. Pareillement, il sera question des réflexes et des actions à mettre en place pour minimiser les risques.

Cet évènement sera animé par Rémy Martin, responsable du développement propme grand sud-est Orange. Cette rencontre sera suivie d'une visite des locaux de l'opérateur historique Orange.

Ecrit par le 3 juillet 2024

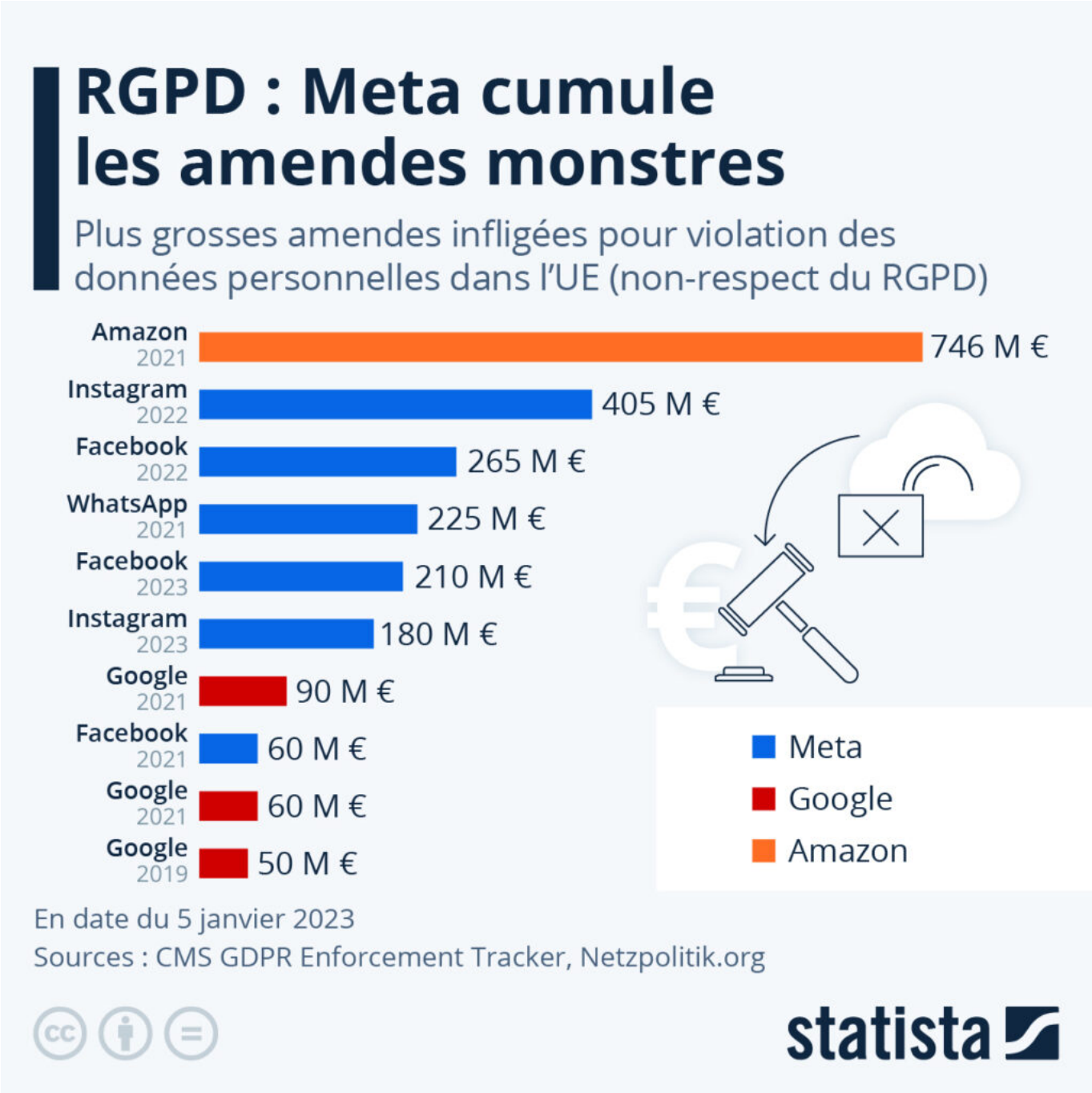
À savoir
De 8h30 à 10h30. 24 mai. Parking gratuit sur site. Avenue de la croix rouge. Avignon. Inscription définitive via l'e-mail contact@cpme84.org . 04 90 14 90 90.

J.G

Violation des données : Meta cumule les amendes monstres

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024



Après plusieurs amendes en 2022, Meta débute 2023 avec de nouvelles sanctions. La Commission irlandaise de protection des données, l'équivalent de la Cnil en France, a décidé d'infliger deux lourdes amendes au groupe dirigé par Mark Zuckerberg pour violation du règlement général sur la protection des données (RGPD). Dans le détail, la première, d'un montant de 210 millions d'euros, revient à Facebook, et la seconde, de 180 millions d'euros, concerne Instagram. Dans un communiqué, le

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

régulateur irlandais a expliqué que l'entreprise avait violé « ses obligations en matière de transparence » et se fondait sur une base juridique erronée « pour son traitement des données à caractère personnel à des fins de publicité ».

Comme le montre notre graphique basé sur le suivi de CMS.Law, Meta est désormais représenté par six entrées dans le top 10 des plus grosses sanctions infligées dans le cadre du RGPD dans l'UE. Cumulées, ces six amendes représentent un total de plus de 1,3 milliard d'euros. Outre Meta, Google est également présent dans ce classement avec trois entrées. Le record de l'amende la plus élevée revient toutefois à Amazon, qui a reçu une sanction de 746 millions d'euros en 2021 pour « non-respect des principes généraux de traitement des données ».

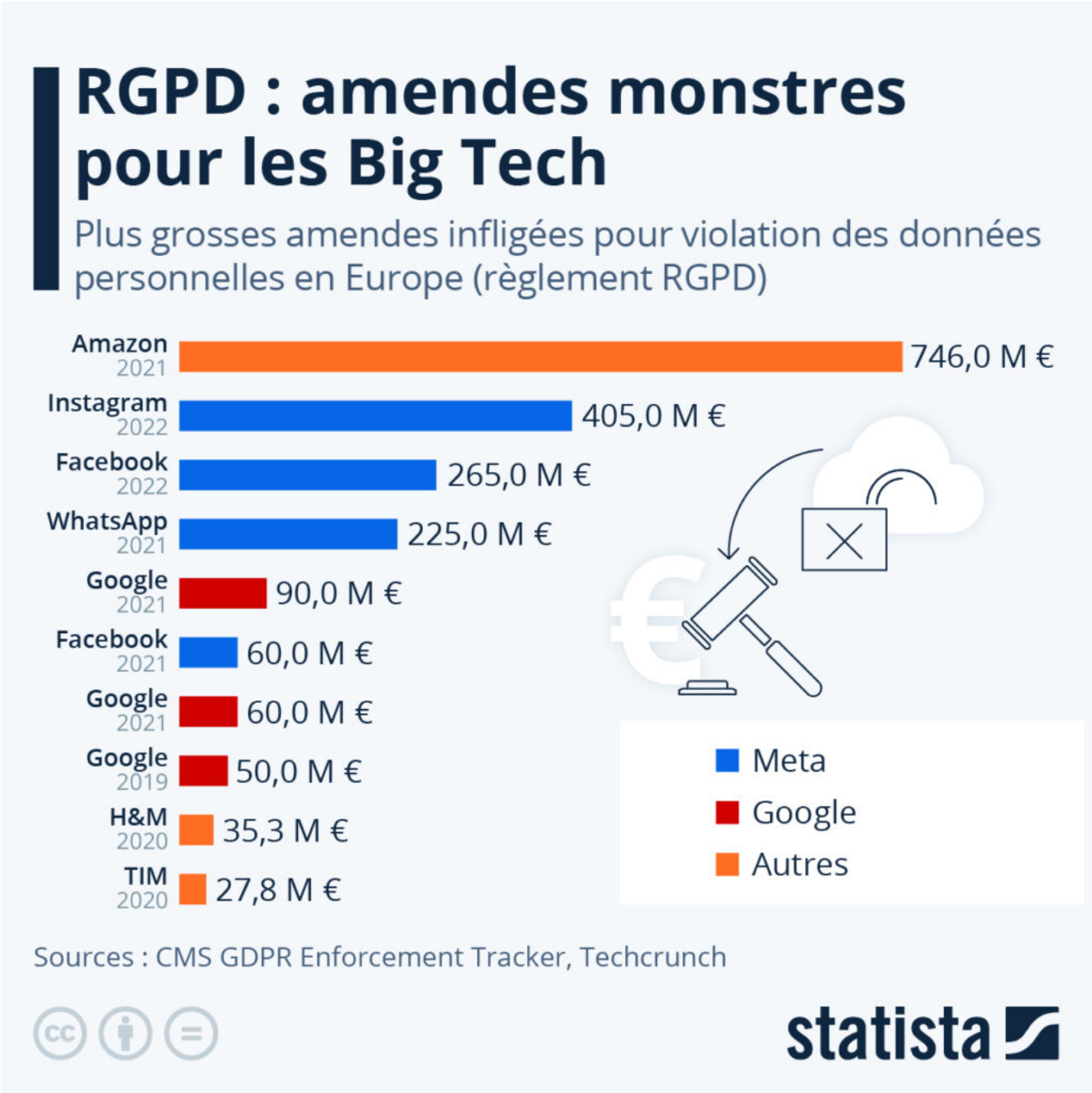
Le cadre réglementaire du RGPD vise à donner aux utilisateurs un plus grand contrôle sur leurs données personnelles et impose de nouvelles normes à la gestion des données en entreprise. Pour les contrevenants à ces règles, les sanctions sont souvent lourdes. Le RGPD a été mis en place le 25 mai 2018, en remplacement de la directive européenne sur la protection des données de 1995, et contient 99 articles. À ce jour, le suivi de CMR.Law recense plus de 1 500 violations individuelles du RGPD, bien que les données soient très probablement incomplètes puisque toutes les amendes ne sont pas rendues publiques.

De Tristan Gaudiaut pour Statista

Violation des données : les amendes monstres infligées aux Big Tech

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024



La Commission irlandaise de protection des données, l'équivalent de la Cnil en France, a décidé la semaine dernière d'infliger une amende de 265 millions d'euros à Facebook pour avoir violé le règlement général sur la protection des données (RGPD), suite à une immense fuite de données d'utilisateurs survenue entre mai 2018 et septembre 2019. Cette amende est la quatrième infligée aux plateformes détenues par la société mère de Facebook, Meta. Même si cette somme peut sembler considérable, il ne

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

s'agit pas du montant le plus élevé qu'une entreprise ait dû payer dans l'histoire du RGPD.

Comme le montre le graphique ci-dessus, cet honneur discutable revient à Amazon, un autre géant du Web. En juillet 2021, le régulateur luxembourgeois avait infligé une amende monstre de 746 millions d'euros à la branche européenne du groupe américain, pour « non-respect des principes généraux de traitement des données dans le cadre du RGPD », d'après le suivi réalisé par CMS. La quatrième place de ce classement revient à la messagerie WhatsApp, suivie de trois amendes reçues par Google et d'une infligée à Facebook.

Le cadre réglementaire du RGPD vise à donner aux utilisateurs un plus grand contrôle sur leurs données et impose de nouvelles normes à la gestion des données personnelles en entreprise. Pour les contrevenants à ces règles, les sanctions sont souvent lourdes. Le RGPD a été mis en place le 25 mai 2018, en remplacement de la directive européenne sur la protection des données de 1995, et contient 99 articles. À ce jour, le suivi de CMR recense 1 507 violations individuelles du RGPD, bien que les données soient très probablement incomplètes puisque toutes les amendes ne sont pas rendues publiques.

Tristan Gaudiaut pour Statista.

Télétravail en vacances, comment protéger vos données

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

Les Tracances, la nouvelle tendance du télétravail en vacances. D'après une enquête menée par le cabinet Génie des lieux et publiée le 11 juillet dernier, 35 % des travailleurs français déclarent qu'ils feront du télétravail depuis leur lieu de vacances cet été. Parmi eux, 24 % se limiteront à 1 ou 2 jours par semaine afin de profiter de leurs proches, tandis que 11 % le feront à temps plein.

Voyager tout en travaillant, c'est pouvoir changer de bureau chaque jour, profiter de paysages d'exception pendant sa pause-café mais aussi s'exposer à des risques en matière de cybersécurité. Pour partir tranquille, en plus de penser à prendre l'anti-moustique dans la valise, le digital nomad doit veiller à la protection de ses données.

Eviter de se connecter depuis un lieu public

Loin du bureau, le digital nomad doit éviter de se connecter en Wi-Fi dans un lieu public complètement ouvert comme une gare ou un café. Ces réseaux comportent de multiples failles de sécurité. Celles-ci peuvent entraîner une fuite des données contenues dans l'ordinateur, dont celles stockées sur le réseau de l'entreprise et qui sont souvent confidentielles. Cela revient à laisser la porte grande ouverte à des intrusions malveillantes. Il en est de même dans les espaces de coworking. Même s'ils paraissent plus sécurisés, les connexions dans ces lieux ne bénéficient généralement pas d'un niveau de sécurité suffisant. De plus, le digital nomad s'expose à des risques de vol ou perte de matériel (disque dur, clé USB…), qui pourraient compromettre gravement la sécurité des données.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

Utiliser des équipements fiables
Il est déconseillé d'utiliser un équipement personnel pour travailler. En effet, ce dernier n'a pas bénéficié des configurations de sécurité nécessaires : authentification au démarrage, chiffrement des disques, gestion des droits administrateurs ou de la connexion à des supports amovibles… Ces contrôles doivent être effectués par l'entreprise sur l'équipement professionnel avant de laisser partir le digital nomad, que ce soit à l'étranger ou dans sa maison de campagne. Objectif : protéger les accès aux données.

Préserver la confidentialité des échanges
Le digital nomad entretient des liens constants avec son entreprise. Pour cela, il utilise des outils de visioconférence pour ses réunions, ses appels et aussi ses partages de fichiers. Là encore, la vigilance est de mise. Des protections physiques peuvent être utiles, comme des filtres écrans ou des verrous de ports USB qui empêchent tout regard indiscret ou intrusion dans le système. Aujourd'hui, la plupart des échanges en vidéoconférence sont susceptibles d'être écoutés et regardés. En dehors du bureau, ce risque d'espionnage informatique est encore plus élevé. Il peut entraîner des conséquences graves pour l'intégrité des salariés et des données de l'entreprise. Les entreprises ont donc intérêt à faire le choix d'une solution de visio collaboration sécurisée.

Vous avez dit cyber sécurité ?
L'ANSSI les accompagne dans leur choix via un processus de certification et de qualification. Elle identifie ainsi les solutions de cybersécurité les plus fiables, en leur attribuant un label « Visa de sécurité ».

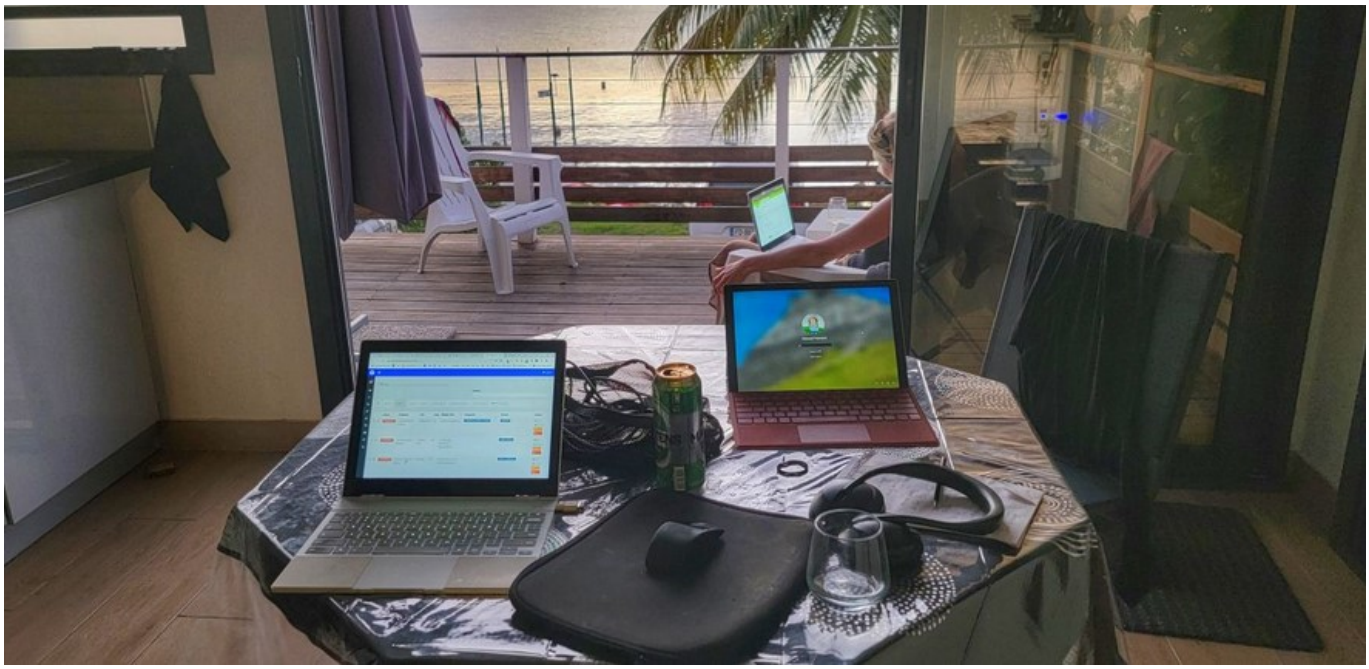
VPN oui, mais pas que…
Ne pas se contenter de l'utilisation d'un VPN : Le VPN constitue un lien sécurisé entre l'équipement du salarié en voyage et le réseau de son entreprise. Mais il ne protège pas des failles de sécurité. Si le télétravailleur se connecte à un réseau Wi-Fi public et laisse entrer par mégarde un logiciel malveillant sur son ordinateur, le virus pourra s'infiltrer via le VPN et remonter jusqu'au serveur de l'entreprise…

Prendre garde à ses propres données personnelles
Qui dit digital nomad dit passeport, billets d'avion ou de trains qui sont parfois partagés dans les messageries des outils de visiocollaboration. Ces données personnelles sont exposées si les échanges ne sont pas sécurisés, ce qui peut entraîner une usurpation d'identité.

Sources
Cet article provient de Tixeo secure video conferencing. D'après une enquête **menée par le cabinet Génie des lieux et publiée le 11 juillet dernier**. Renaud Ghia, Président de Tixeo, le leader européen de la visioconférence sécurisée et l'unique technologie de visioconférence à être certifiée et qualifiée par l'ANSSI (Agence nationale de la sécurité des systèmes d'information), a offert ces conseils.
MH

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024



DR

---

10 conseils pour vous protéger pendant vos vacances contre les cybermenaces

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

Si vous faites partie de ces vacanciers qui ne partent jamais sans leurs objets connectés, méfiez-vous des menaces lorsque vous utilisez un Wi-Fi public pour vous connecter à votre banque en ligne, boutique en ligne ou tout simplement pour vérifier vos e-mails.
Eset, spécialisé dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public, propose un guide pour vous permettre de voyager en toute sécurité et garder ainsi toutes vos données personnelles et vos appareils protégés.

1. Avant de prendre la route, assurez-vous d'exécuter sur vos appareils une mise à jour complète du système d'exploitation ainsi que des logiciels, et de posséder une solution de sécurité de confiance.

2. Sauvegardez vos données et placez-les dans un endroit sûr. Pensez à déplacer les données sensibles du disque dur de votre ordinateur portable sur un disque dur externe chiffré le temps de vos vacances.

3. Ne laissez jamais vos appareils sans surveillance dans les lieux publics. Activez la fonction antivol de vos appareils pour tracer les appareils volés ou perdus, et au besoin d'effacer les contenus à distance.

4. Mettez un mot de passe fort et activez la fonction 'délai d'inactivité' sur tous vos appareils, que ce soit votre ordinateur portable, votre tablette ou votre téléphone. Retrouvez tous les conseils d'Eset pour un

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024

mot de passe efficace en cliquant ici.

5. Dans la mesure du possible, utilisez uniquement des accès internet de confiance. Demandez à votre hôtel ou l'endroit où vous logez le nom de leur Wi-Fi et utilisez exactement le même nom : faites attention aux arnaques qui essaient de ressembler aux Wi-Fi publics en ajoutant le mot « gratuit » au nom de la connexion Wi-Fi.

6. Si l'Internet de votre hôtel vous demande de mettre à jour un logiciel afin de pouvoir vous connecter, déconnectez-vous immédiatement et informez-en la réception.

7. Ne vous connectez pas à des connexions Wi-Fi qui ne sont pas chiffrées avec WPA2. Toutes les normes inférieures à celle-ci ne sont tout simplement pas assez sûres et peuvent être facilement piratées.

8. Si vous devez utiliser le Wi-Fi public pour vous connecter à votre réseau d'entreprise, utilisez toujours votre VPN (réseau virtuel privé).

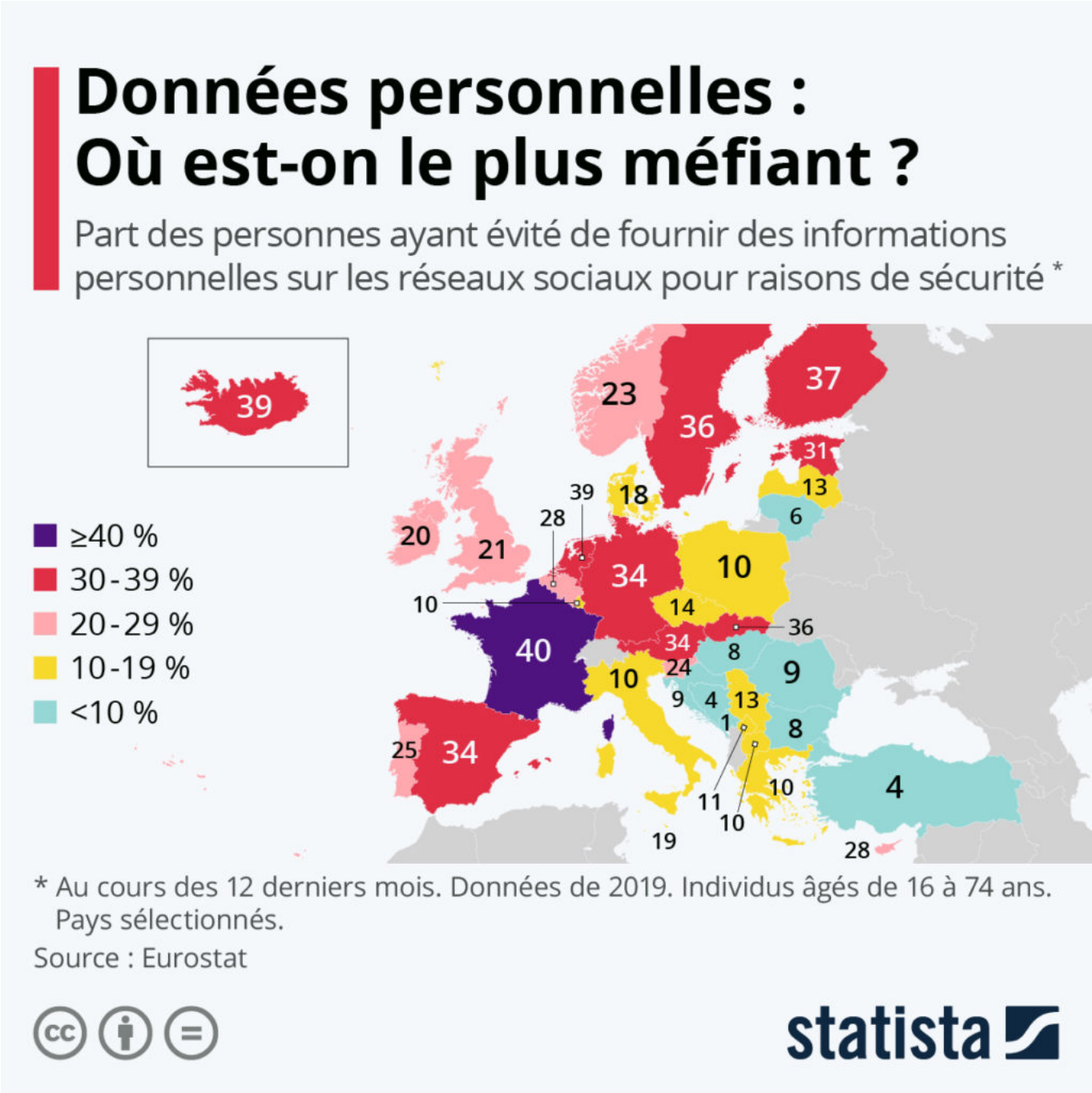
9. Si ce n'est pas urgent, évitez les banques et boutiques en ligne quand vous utilisez le Wi-Fi public. Sinon, nous vous conseillons d'utiliser le partage de connexion de votre téléphone et de surfer en utilisant internet sur votre téléphone portable.

10. Si vous n'utilisez pas encore d'antivirus de confiance et suspectez votre ordinateur portable d'être infecté, vous pouvez utiliser gratuitement le scanner ESET Online qui ne nécessite aucune installation et peut être utilisé pour détecter et retirer des logiciels malveillants.

Données personnelles : les Français sont les plus méfiants

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 3 juillet 2024



Le monde passe en moyenne près de 7 heures par jour connecté à Internet. En ce moment même, une quantité énorme de données, souvent de nature privée, transite sur la toile, et le nombre de personnes préoccupées par la sécurité de leurs données personnelles ne cesse d'augmenter.

Selon les données d'Eurostat, un citoyen européen sur quatre a déclaré avoir évité de fournir des

Ecrit par le 3 juillet 2024

informations personnelles sur les réseaux sociaux ou professionnels en 2019 pour des raisons de sécurité. Comme dans un certain nombre d'autres domaines, ce sont les Français qui se montrent les plus méfiants. 40 % des personnes interrogées en France ont préféré ne pas fournir de données personnelles sur une plateforme par crainte de sécurité, soit le pourcentage le plus élevé de l'étude. Parmi les plus inquiets à ce sujet, on retrouve ensuite les Pays-Bas (39 %), la Finlande (37 %), ainsi que la Slovaquie et la Suède (36 % chacun).

En revanche, la question des données personnelles semble moins préoccupante dans les pays d'Europe de l'Est, où un pourcentage beaucoup plus faible de la population déclare s'être abstenu de fournir de telles informations : 9 % en Croatie et Roumanie, 8 % en Bulgarie et Hongrie, 6 % en Lituanie.

Sur le même sujet : vous pouvez consulter notre graphique sur les applications qui partagent le plus de données avec des tiers.

De Tristan Gaudiaut pour Statista