Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

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
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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

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

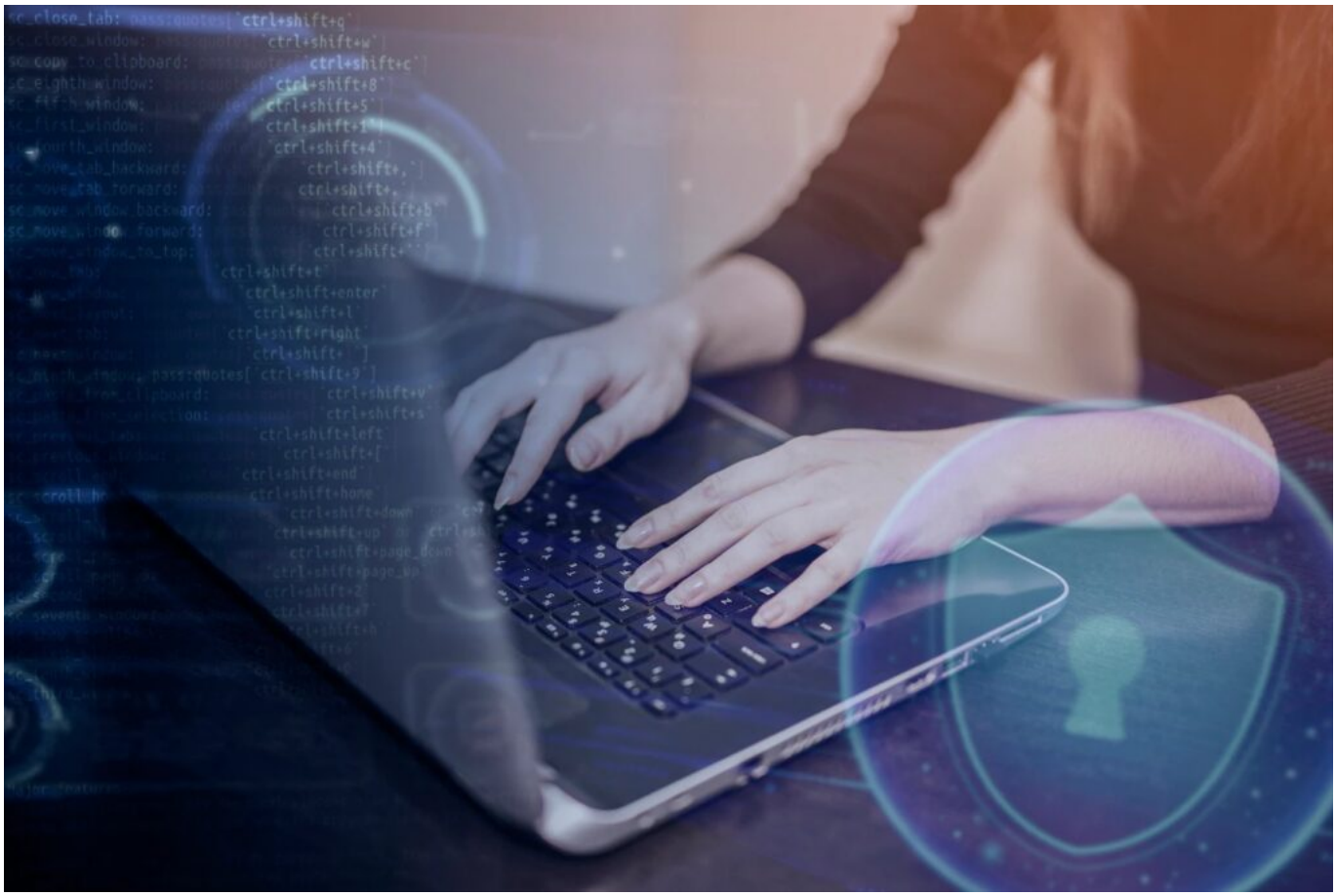
« Informatique et libertés » : une loi en avance sur son temps !
Quels sont dans les années 1970 les principaux problèmes posés par l'avènement de l'informatique concernant la protection des données et des libertés ? Qu'est-ce que le projet SAFARI ? Pourquoi la commission informatique et libertés a-t-elle été créée ? Quelle est la mission de la CNIL ? A écouter

L.G.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

La CPME 84 organise un petit-déjeuner sur la cybersécurité



La CPME 84 s'engage pour prévenir les cyberattaques au sein des entreprises. L'entité vauclusienne se joint au comité local des banques du Vaucluse pour organiser le mardi 26 mars de 8h30 à 10h30 un petit-déjeuner thématique sur la cybersécurité à l'Ecomin d'Avignon.

Selon le rapport du Baromètre Euler Hermès publié en 2021, 2/3 des entreprises ont déjà subi au moins une tentative de fraude. Un constat inquiétant qui vient confirmer une tendance de plus en plus menaçante, les cyberattaques ne cessent de se multiplier et touchent les entreprises de tous les horizons, de petites ou moyennes tailles.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Pour y faire face et les prévenir, la CPME 84 organise en collaboration avec le comité local des banques du Vaucluse un petit-déjeuner autour du sujet des cyberattaques et de la lutte contre la fraude en entreprise.

L'évènement, qui se déroulera ce mardi 26 mars de 8h30 à 10h30 à l'Ecomin d'Avignon, sera animé par Franck Chemin, responsable du service cybersécurité du Crédit Agricole Alpes-Provence, et Frédéric Soufflet, responsable flux du Banque Populaire Méditerranée. Les deux hommes pourront apporter leur expertise et leurs solutions pour se protéger face à ces atteintes financières. Cette matinée accueillera également un représentant régional de la Police Judiciaire.

51 types de cyberattaques

Avec la démocratisation du digital et du numérique qui prend chaque jour de plus en plus d'ampleur au sein des entreprises et la pratique du télétravail qui est devenue une tendance quasi systémique, les escroqueries financières sont désormais légion. En 2022, les préjudices recensés sur la fraude au président s'élevaient à 313 millions d'euros, soit trois fois plus qu'il y a 5 ans.

Cybersurveillance.gouv.fr compte 51 types de modes opératoires qui reviennent constamment. Parmi les fraudes les plus citées par les entreprises et PME, on compte la fraude au R.I.B qui représentent 45% des cyberattaques et arnaques, la fraude au président (41%), l'intrusion dans le système informatique (41%), les usurpations d'identité (banque, avocat, assurance) à hauteur de 30% et enfin la fraude aux faux conseillers bancaires.

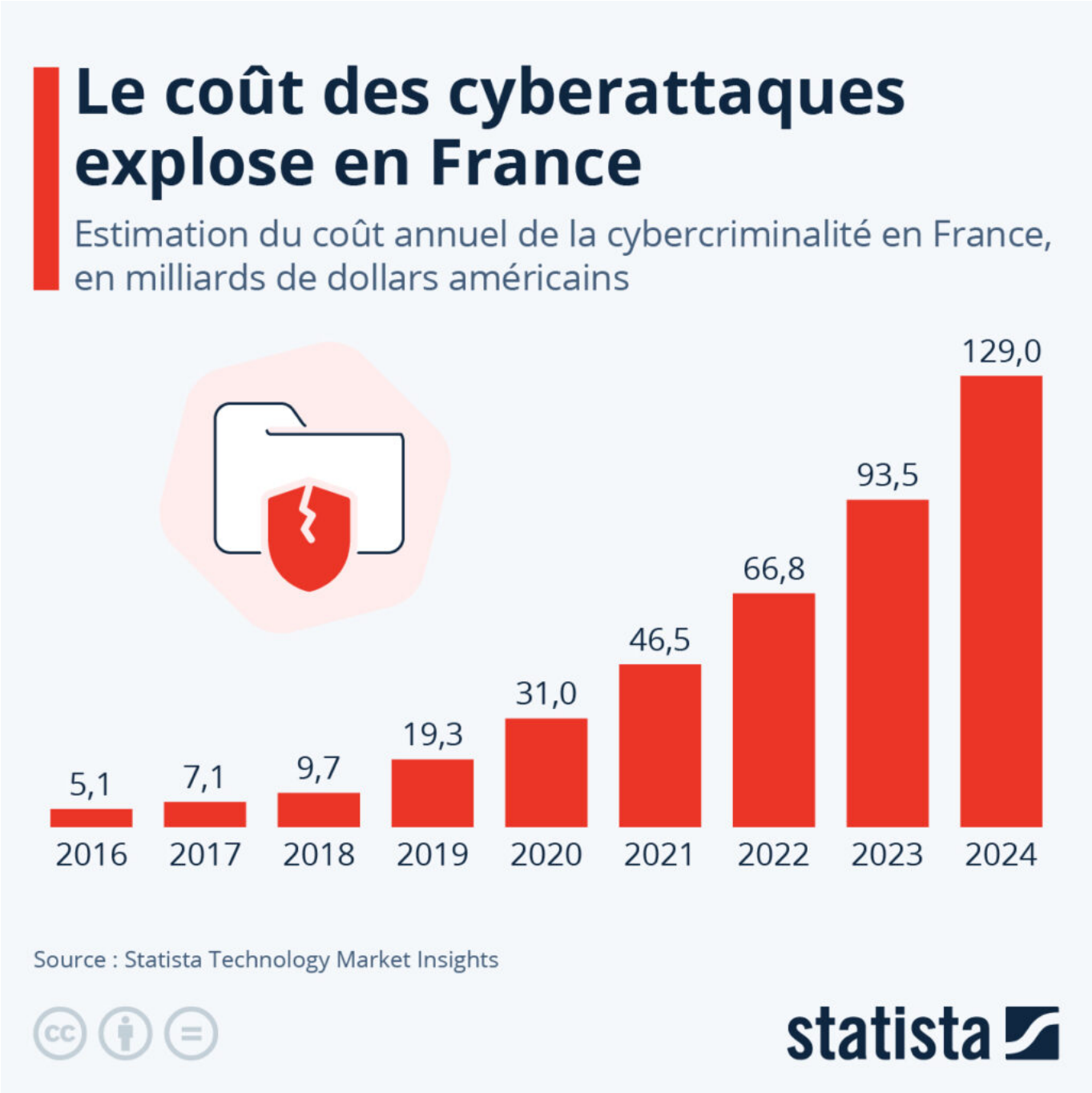
Infos pratiques : Petit-déjeuner « Cybersécurité et lutte contre la fraude en entreprise ». Ecomin d'Avignon. 135 avenue Pierre Semard, 84000 Avignon. Mardi 26 mars 2024 de 8h30 à 10h30. Inscription par mail à cette adresse : contact@cpme84.org

---

Le coût de la cybercriminalité explose en France

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Le coût annuel de la cybercriminalité en France est aujourd'hui évalué à plus de 100 milliards d'euros. Selon les dernières estimations issues des Technology Market Insights de Statista, le coût total des cyberattaques et autres actes malveillants en ligne devrait atteindre 129 milliards de dollars américains dans le pays en 2024 (soit environ 119 milliards d'euros), contre près de 94 milliards de dollars l'an passé.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Comme le retrace notre infographie, le coût de la cybercriminalité en France a littéralement explosé ces huit dernières années. En 2016, ce chiffre n'était évalué qu'à 5,1 milliards de dollars, avant de connaître une hausse moyenne de plus de 30 % chaque année. Cette tendance va de pair avec la multiplication, la diversification et le perfectionnement des cyberattaques au cours de la période étudiée.

D'après l'édition 2024 du baromètre du CESIN, près d'une entreprise française sur deux a été victime d'une cyberattaque avec un impact significatif l'an dernier. En outre, le cyberespionnage représenterait un risque élevé pour deux entreprises sur cinq (toutes industries confondues). Les auteurs du rapport soulignent notamment « la complexité croissante du paysage de la cybersécurité, avec des attaquants qui ajustent leurs tactiques ».

De Tristan Gaudiaut pour Statista

CCI de Vaucluse : conférence sur la cybersécurité

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



À l'occasion de la Semaine de l'industrie, qui a lieu du 27 novembre au 3 décembre, la Chambre de commerce et d'industrie (CCI) de Vaucluse organise une conférence participative sur la cybersécurité sur son campus ce vendredi 1er décembre, 'Venez découvrir comment un hacker décide de vous cibler'.

Animée par les étudiants en master cybersécurité de la CCI de Vaucluse, médaillés d'argent aux Worldskills France, la conférence accueillera le témoignage de l'entreprise carpentrassienne Thucy, spécialisée dans la sécurité informatique.

La cybersécurité est essentielle, que ce soit pour les grandes entreprises ou pour les très petites entreprises, qui s'exposent à des personnes mal intentionnées, qu'elles disposent de secrets industriels ou non. La conférence mettra en avant les risques auxquels les entreprises peuvent être confrontées, pourquoi elles doivent s'en protéger, et surtout comment.

Inscription via le formulaire en ligne.
Vendredi 1er décembre. De 8h30 à 11h. Amphithéâtre du Campus de la CCI de Vaucluse. Allée des Fenaisons. Avignon.

V.A.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

5 conseils pour voyager en toute sécurité cet été



Les vacances d'été font de vous la proie idéale des hackers. Évitez cette fâcheuse situation grâce à ces 5 conseils de cybersécurité.

Les voyages d'été approchent et vous planifiez vos vacances bien méritées ? De simples actions telles que l'utilisation du Wi-Fi public dans les aéroports, les hôtels ou les lieux touristiques peuvent rendre vos appareils vulnérables au piratage et compromettre votre cyber-identité. Pour vous aider à protéger votre identité, vos données financières, vos documents sensibles et vos mots de passe, voici 5 bonnes pratiques en matière de cybersécurité à adopter cet été.

1. Limitez les messages sur les réseaux sociaux qui mentionnent votre destination
Les posts sur les réseaux sociaux sont devenus l'activité préférée des voyageurs. Cependant, il peut être dangereux de publier des messages pendant que vous voyagez et de divulguer votre position exacte alors que vous êtes encore sur place. Une fois que votre position est exposée publiquement, n'importe quel

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

acteur malveillant peut vous prendre pour cible. Bien que cela puisse sembler improbable en tant que touriste, les locaux qui connaissent mieux votre environnement auront plus de facilité à vous localiser que vous ne le pensez. Si vous êtes toujours tenté de publier, attendez d'avoir déménagé dans une nouvelle destination ou mieux encore, le moment où vous serez rentré chez vous.

2. Évitez les réseaux Wi-Fi publics
Bien qu'il puisse être difficile de trouver un réseau Wi-Fi fiable lors d'un voyage, il vaut mieux être en sécurité que dangereusement connecté aux réseaux Wi-Fi publics. Les attaquants peuvent utiliser ce que l'on appelle une attaque de type « man-in-the-middle » (MITM) lorsque votre appareil est connecté à un réseau Wi-Fi public, ce qui permet aux hackers d'accéder à votre navigateur ou à votre application et de récupérer vos données stockées. En règle générale, les réseaux Wi-Fi publics doivent toujours être évités.

3. Envisagez d'utiliser un VPN
Lorsque vous voyagez, l'utilisation d'un réseau privé virtuel (VPN) vous permet de rester protégé lorsque vous vous connectez depuis n'importe quel endroit. Non seulement un VPN vous permet d'éviter la limite de bande passante, mais il protège également votre identité en ligne et sécurise votre connexion depuis n'importe quel endroit, même si vous vous trouvez sur un tout autre continent.

4. Téléchargez les documents importants pour les sauvegarder
Voyager vers des destinations et des attractions touristiques nouvelles et inconnues peut être chaotique, ce qui augmente le risque de vol ou d'égarement d'effets personnels importants (passeports, visas, dossiers médicaux, etc.). En téléchargeant des copies de ces documents importants contenant des informations très sensibles vers un gestionnaire de mots de passe sécurisé, vous disposerez de copies numériques de sauvegarde en cas de perte ou de vol.

5. Partagez en toute sécurité des informations d'urgence avec une source de confiance
Pendant vos vacances, renforcez votre sécurité en partageant des informations importantes avec des membres de votre famille ou des amis de confiance, afin qu'ils puissent y accéder en cas d'urgence. Utilisez un service chiffré pour partager en toute sécurité des informations d'assurance ou des documents d'identité, comme votre passeport, pour une durée limitée. Ainsi, en cas d'urgence médicale ou autre, il pourra vous aider sans que des informations sensibles soient exposées par mail, SMS ou messagerie, même à l'autre bout du monde.

Arnaud De Backer, Channel Sales Manager EMEA, Chez Keeper Security.

Stoïk s'étend dans le Sud-Est et nomme

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Alban Dupin responsable du développement courtage



Stoïk, l'assurance qui couvre et protège des cyberattaques vient de nommer Alban Dupin en tant que responsable du développement courtage pour couvrir le Sud-Est de la France et le littoral méditerranéen. Après plusieurs années dans le milieu de l'assurance au sein de l'entreprise Allianz France puis chez GAN Assurances, Alban Dupin aura pour mission d'animer un réseau de courtier local et de les accompagner dans la distribution du produit d'assurance cyber de Stoïk.

> "Après avoir découvert l'assurance grand public et le marché des professionnels, je suis très heureux de rejoindre les équipes de Stoïk et de me spécialiser dans le produit d'assurance cyber dans un contexte où le marché gagne fortement en maturité."
>
> *Alban Dupin*

En France, seulement 10% des ETI sont assurées contre 94% pour les grandes entreprises. Et le chiffre

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

est encore plus bas pour les moyennes entreprises et les petites et micro-entreprises. Mais une cyberattaque peut concerner n'importe quelle entreprise, peu importe sa taille. C'est dans ce cadre que Stoïk, première assurance spécialisée sur le risque cyber en Europe, poursuit son expansion en région.

V.A.

Quelles sont les bonnes pratiques à adopter sur internet pour la sécurité de vos enfants ?



Lionel Paris, expert produits réseau pour Netgear, explique comment gérer la connexion à

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

internet de vos enfants pour une tranquillité d'esprit de tous les membres de la famille.

En quelques années, internet et les réseaux sociaux ont pris une place importante dans notre quotidien. Mais cet univers digital est loin d'être à l'abri des dangers, c'est pour cela que transmettre de bons réflexes à nos enfants dès le plus jeune âge est primordial. Optez en premier lieu pour un contrôle parental pour permettre à vos enfants et adolescents de rester connectés tout en étant protégé.

Gérez le temps d'écran de vos enfants
Grâce au contrôle parental, vous pourrez contrôler la connexion internet de vos enfants. Il est important pour un enfant ou un adolescent de savoir gérer son temps en ligne et ne pas devenir dépendant à l'utilisation d'internet. Grâce à un contrôle parental, il vous sera possible de suspendre volontairement internet sur les appareils connectés de vos enfants lors de moments tels que les études ou encore les heures des repas.

Surveillez les contenus publiés et visionnés
Internet est un univers impitoyable, on y trouve tout mais surtout n'importe quoi. Malgré tous ses avantages, internet reste rempli de sites dangereux et frauduleux, qui véhiculent de fausses informations ou incitent à la haine. Entre exposition à des images choquantes ou cyberharcèlement, ne prenez pas de risques pour la santé mentale de votre enfant. Grâce à un contrôle parental optimal, obtenez des informations sur l'activité de vos enfants en ligne et sur l'historique, définissez des filtres et bloquez les sites inappropriés. Rendez l'expérience de vos enfants en ligne sécurisée et apaisante.

Offrez-leurs des habitudes saines
L'importance pour vos enfants est de garder des habitudes saines pour promouvoir un équilibre entre le temps en ligne et le temps hors-ligne. Pour cela, choisissez les filtres de contenu les plus adaptés à l'âge de vos enfants, définissez des limites d'accès aux jeux ou aux réseaux sociaux, planifiez des heures de sommeil pour éviter le téléphone caché sous l'oreiller et prévoyez des temps d'arrêt sans avoir à leur confisquer leurs appareils.
L'importance est d'accompagner les enfants dans leurs expériences sur internet, en leur expliquant ses dangers, pour leur transmettre de bons réflexes et limiter leur dépendance sans les frustrer. Grâce au contrôle parental, vous pourrez construire des habitudes saines et protéger votre enfant sans le priver de rester connecté.

Lionel Paris, expert produits réseau pour Netgear

Cybersécurité : les collectivités vauclusiennes

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

ne sont pas à l'abri



La section départementale de Vaucluse du Syndicat des directeurs généraux des collectivités territoriales (SNDGCT) vient d'organiser une rencontre sur le thème de la cybersécurité. L'occasion pour Kevin Heydon, délégué à la sécurité numérique de l'Anssi en Paca et en Corse, ainsi que Karine Icard, présidente du SNDGCT 84*, de sensibiliser sur les risques de cyberattaque sur le secteur public.

Paralysie des services, pertes de données essentielles : le secteur public est aujourd'hui de plus en plus la cible des cyberattaquants. En 2020, en France, 30% des collectivités territoriales ont été victimes d'une attaque de type rançongiciel (envoi d'un logiciel malveillant de chiffrage des données de quelqu'un dans le but de lui extorquer de l'argent). Un chiffre en hausse de 50 % par rapport à 2019 selon une étude du Clusif. Pour autant, il y encore peu de temps la cybersécurité ne semblait pas encore être une préoccupation centrale des collectivités territoriales. Ainsi, selon un sondage Ifop pour l'Observatoire des politiques publiques réalisé en janvier 2020, seuls 33 % des fonctionnaires territoriaux interrogés déclaraient que leur organisation avait mis en place un programme de cybersécurité.

Depuis, la mobilisation des associations d'élus et structure d'agents territoriaux comme le SNDGCT

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

notamment a permis une certaine prise de conscience des collectivités territoriales. Ces dernières tâchent donc maintenant de se prémunir au mieux face à ce phénomène expansionniste avec des pratiques numériques réinterrogées, des actions de sensibilisation, un risque numérique intégré au plan de continuité d'activité, etc.

Dans cette logique, l'Association des maires de France (AMF) a ainsi édité en novembre 2020 un guide intitulé 'Cybersécurité : toutes les communes et les intercommunalités sont concernées' regroupant une trentaine de recommandations et de bonnes pratiques en matière de sécurité numérique. De son côté, le sénat s'est également penché sur cette problématique, en octobre dernier, lors d'une table-ronde sur 'Les collectivités territoriales face au défi de la cybersécurité'.

> **« La question n'est plus de savoir 'si' les collectivités seront la cible d'une cybermalveillance, mais plutôt 'quand'. »**

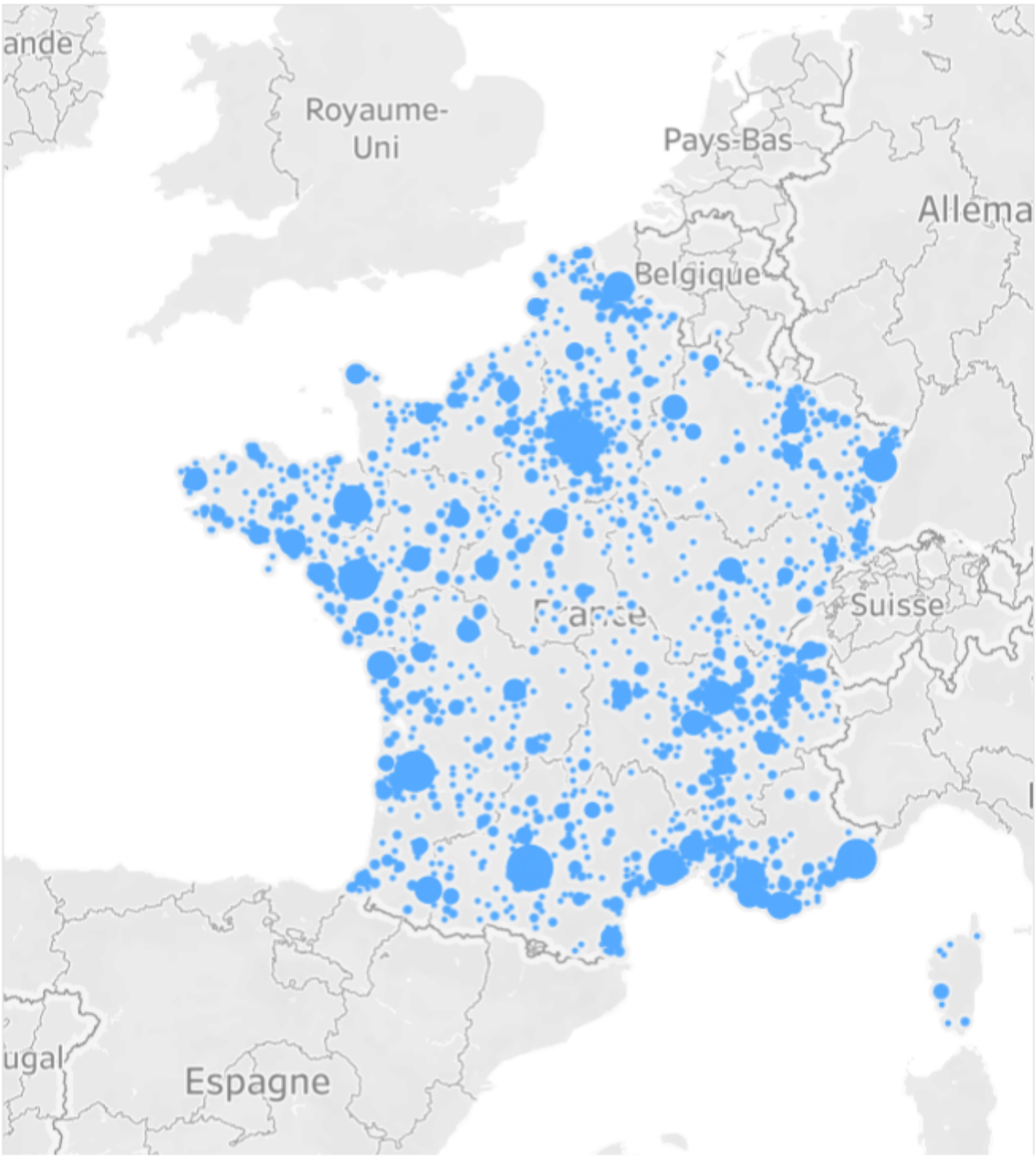
« L'objectif des cyberattaquants est de capter de la donnée, de la bloquer et ce, à des fins lucratives. Aujourd'hui, la question n'est plus de savoir 'si' les collectivités seront la cible d'une cybermalveillance, mais plutôt 'quand' », expliquent Karine Icard, présidente du SNDGCT 84 et directrice générale des services de la Communauté d'agglomération Luberon Monts de Vaucluse, ainsi que Kevin Heydon, délégué à la sécurité numérique de l'Anssi en Paca et en Corse, lors de la rencontre de sensibilisation 'Cybersécurité : les collectivités territoriales du Vaucluse en parlent…' qui vient de se tenir dans les locaux du syndicat des eaux Durance Ventoux à Cheval-Blanc.

Un nouveau fléau

« Ce nouveau fléau peut entraîner une paralysie des services publics, entacher lourdement l'image même de ces derniers et engendrer des dépenses élevées », poursuivent les organisateurs de ce rendez-vous auquel a participé une trentaine de dirigeants provenant de communes, d'intercommunalités ou de syndicats du territoire de Vaucluse.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026



Source : Cybermalveillance.gouv.fr, 2021

Localisation des collectivités territoriales françaises ayant été victime d'une attaque au rançongiciel en 2020.

Au travers des témoignages des directeurs généraux des services, Emmanuel Bohn de la Communauté de communes du Pays d'Apt et Vincent Rey de la ville de Morières-lès-Avignon, dont les collectivités ont été

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

victime « de perte totale de leurs données nécessitant une reconstruction longue de leur système d'information », les participants ont pu ensuite travailler autour de la notion du risque numérique en s'interrogeant sur les moyens pour s'en prémunir, les bonnes pratiques à déployer, les leviers à activer ou bien encore les bons réflexes à avoir en cas de cyberattaque ?

La piste d'une protection collective ?

Bien souvent, le manque de budget et de personnes qualifiées justifie en partie les difficultés des collectivités territoriales en matière de cyberprotection de leurs outils et données numériques.

« Faute de temps mais également de compétences et de ressources humaines qualifiées, les petites communes se contentent parfois d'installer ponctuellement un anti-virus, alors que la cybersécurité doit être mise à jour en permanence, constatent les travaux du sénat. Or, la pénurie de compétences est telle que l'Anssi a lancé un 'observatoire des métiers de la cybersécurité' afin d'aider les acteurs concernés dans leur politique de recrutement et de formation. Dans ce contexte, la mutualisation au plus près des collectivités concernées s'avère être un choix judicieux pour mettre en commun les efforts, affronter les pénuries de professionnels qualifiés et ainsi mettre en place une protection collective. »

Pour cela, les responsables et DGS des collectivités de Vaucluse peuvent ainsi compter sur le l'accompagnement de l'Anssi et du SNDGCT 84 des acteurs territoriaux dans la sécurisation de leur développement numérique.



Le SNDGCT 84 et l'Anssi lors de la rencontre de sensibilisation sur le thème 'Cybersécurité : les collectivités territoriales du Vaucluse en parlent…' qui s'est tenue dans les locaux du syndicat des eaux Durance Ventoux à Cheval-Blanc.

**Le SNDGCT a été créé en 1948. L'organisation professionnelle compte aujourd'hui près de 4 000 adhérents au niveau national. Elle se compose d'Unions régionales, elles-mêmes divisées en Sections*

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

départementales. Karine Icard est présidente de la section départementale de Vaucluse depuis septembre 2020. Autour d'elle, un bureau avec 3 membres, Gilles Meunier, directeur général adjoint de la Communauté de communes de Pays des Sorgues Monts de Vaucluse, Johanna Quijoux, directrice générale des services de Piolenc et Emmanuelle Licitri, directrice générale adjointe mutualisée Ville de Cavaillon et Luberon Monts de Vaucluse Agglomération.

Scannez avec prudence, les arnaques aux QR codes fleurissent



Les QR codes font fureur et les escrocs l'ont remarqué. « Méfiez-vous de ces petits carrés noirs et blancs », prévient Benoit Grunemwald, expert en cybersécurité chez Eset France.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

Les QR codes ont le vent en poupe. Ces modestes carrés existent peut-être depuis 1994, mais ils sont réellement devenus célèbres depuis la crise du Covid-19. Aujourd'hui, vous pouvez les apercevoir partout, les codes étant utilisés pour l'affichage des menus de restaurants jusqu'aux transactions sans contact en passant par des applications de partage de contacts.
Toutefois, comme toute autre technologie courante, l'utilisation généralisée des QR codes a également attiré l'attention des escrocs, à des fins criminelles. Cette tendance a même suscité une alerte de la part du FBI (Federal bureau of investigation) aux États-Unis. Comment les fraudeurs utilisent-ils les codes à des fins illicites ?

Qu'est-ce qu'un QR code et comment fonctionne-t-il ?
Abréviation de 'Quick response', un QR code est un type de code-barres interprétable par une machine instantanément. Un QR code peut contenir jusqu'à 4 296 caractères alphanumériques, ce qui permet un décodage facile par l'appareil photo d'un smartphone.
Les chaînes de texte qui sont codées dans un QR code peuvent contenir une variété de données. L'action déclenchée par la lecture d'un QR code dépend de l'application qui interagit avec ledit code. Les codes peuvent être utilisés pour naviguer vers un site web, télécharger un fichier, ajouter un contact, se connecter à un réseau Wi-Fi et même effectuer des paiements. Les QR codes sont très polyvalents et peuvent être personnalisés pour inclure des logos. Les versions dynamiques des QR codes vous permettent même de modifier le contenu ou l'action à tout moment. Cette polyvalence peut toutefois être une arme à double tranchant.

Comment les QR codes peuvent être exploités ?
Le grand nombre de cas d'utilisation des QR codes (et le potentiel d'utilisation abusive) n'échappe pas aux fraudeurs. Voici comment les cybercriminels peuvent détourner les codes pour voler vos données et votre argent :

1. **Redirection vers un site web malveillant pour voler des informations sensibles :** Les attaques d'hameçonnage ne se propagent pas uniquement par e-mails, des messages instantanés ou des SMS. Tout comme les attaquants peuvent utiliser des publicités malveillantes et d'autres techniques pour vous diriger vers des sites frauduleux, ils peuvent faire de même avec les codes QR.

2. **Téléchargement d'un fichier malveillant sur votre appareil :** De nombreux bars et restaurants utilisent des QR codes pour télécharger un menu au format PDF ou installer une application vous permettant de passer une commande. Les attaquants peuvent facilement falsifier le QR code pour vous inciter à télécharger un fichier PDF malveillant ou une application mobile malveillante.

3. **Déclencher des actions sur votre appareil :** Les QR codes peuvent déclencher des actions directement sur votre appareil, ces actions dépendant de l'application qui les lit. Cependant, il existe certaines actions de base que tout lecteur QR est capable d'interpréter. Il s'agit notamment de la connexion de l'appareil à un réseau Wi-Fi, de l'envoi d'un e-mail ou d'un SMS avec un texte prédéfini, ou de l'enregistrement des informations de contact sur votre appareil. Bien que ces actions ne soient pas malveillantes en soi, elles peuvent être utilisées pour connecter un appareil à un réseau compromis ou envoyer des messages en votre nom.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 2 novembre 2026

4. Détourner un paiement : La plupart des applications financières permettent aujourd'hui d'effectuer des paiements au moyen de codes QR contenant des données appartenant au destinataire de l'argent. De nombreux magasins vous affichent ces codes pour ainsi faciliter la transaction. Cependant, un attaquant pourrait modifier ce QR avec ses propres données et recevoir des paiements sur son compte. Il pourrait également générer des codes avec des demandes de collecte d'argent pour vous tromper.

5. Voler votre identité : De nombreux QR codes sont utilisés comme certificat pour vérifier vos informations, comme votre carte d'identité ou votre carnet de vaccination. Dans ces cas, les QR codes peuvent contenir des informations aussi sensibles que celles contenues dans votre pièce d'identité ou votre dossier médical, qu'un attaquant pourrait facilement obtenir en scannant le QR code.

Nous avons adopté les QR codes dans notre vie quotidienne. Et comme avec toutes les nouvelles pratiques, il nous faut prendre de nouvelles habitudes pour rester vigilants. Chaque nouvelle technologie amène son lot d'avantages mais aussi de menaces.

Benoit Grunemwald, expert en cybersécurité chez Eset France