Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

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 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 ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

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.

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

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

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

Saint-Valentin : attention aux cyber-arnaques

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Avec la Saint-Valentin, les amoureux du monde entier s'efforceront de trouver la meilleure façon de témoigner leurs sentiments. Mais en parallèle, les cybercriminels sembleront également être gagnés par l'esprit de cette journée.

« Comme chaque année, le 14 février, les amoureux célèbreront l'amour à travers le monde,explique Hervé Liotaud, vice-président Europe de l'Ouest chez Sailpoint société spécialisée dans gestion des identités et des accès numérique. Mais ce ne sont pas les seuls pour qui ce jour sera une fête. Les cyber-criminels savent aussi en profiter. Arnaques sur les sites de rencontre, ransomwares, usurpation d'identité, piège au colis… Toutes les techniques seront bonnes pour atteindre leur cible. »

La Saint Valentin : proie des hackers

« En principe, il n'est pas surprenant que les cyber-criminels exploitent des évènements spéciaux tels que des vacances ou des fêtes. Une large cible d'attaque s'ouvre toujours pour des pirates lorsque de nombreuses personnes s'intéressent en même temps à un sujet particulier, et deviennent donc vulnérables. La bonne nouvelle est que les consommateurs ne sont pas sans défense contre ce type d'attaque. »

Des attaques ciblées

« Les précédentes Saint-Valentin ont été fortement marquées par le nombre d'attaques de 'credential stuffing' (vol d'identifiants pour accéder à d'autres comptes) sur les sites de rencontre, dans lesquels des comptes utilisateurs ont été compromis. Les criminels créent régulièrement de faux profils d'utilisateurs avec de faux messages romantiques afin de cibler des personnes seules puis les incitent à leur transférer de l'argent. Chaque année, nous voyons aussi se multiplier les faux sites en ligne proposant une fausse liste de cadeaux mais une escroquerie bien réelle. Cette méthode frauduleuse est particulièrement rentable. Or cette année, une grande part des achats de cadeaux s'effectuera en ligne, les sites marchands en ligne sont d'autant plus susceptibles d'être la cible des cyberattaques. »

Comment s'en protéger ?

« Il est évidemment possible d'appliquer des mesures de sécurité pour atténuer les menaces qui pèsent sur la Saint-Valentin pour protéger les utilisateurs et leurs identités digitales contre ces attaques :

Méfiance lors des achats en ligne : il est primordial de ne faire confiance qu'à des fournisseurs connus et vérifiés, et d'accorder une attention particulière à leur professionnalisme. Ceci inclut, par exemple, la vérification du nom de domaine du site – beaucoup d'acteurs malveillants créent des plates-formes usurpant des noms d'enseignes bien connus, mais ajoutent parfois à la fin « .fr.com » au lieu de simplement « .fr ». Pour s'assurer d'un site authentique, il faut éviter de cliquer directement sur un lien de promotion mais plutôt rechercher la boutique en ligne recherchée sur Google.

Des méthodes de paiement complexes doivent aussi éveiller l'attention : si le paiement doit obligatoirement être fait à l'avance, ceci peut remettre en question le sérieux du site. Des conditions générales de vente très mal traduites et une impossibilité d'impression doivent également alerter les consommateurs, et les inciter à ne pas acheter.

Concernant l'usage des sites de rencontres : les utilisateurs doivent limiter leurs visites à des sites

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

reconnus, et toujours garder à l'esprit que les cyber-criminels les utilisent aussi. En conséquence, lors des communications avec d'autres utilisateurs, il est essentiel de s'assurer qu'ils possèdent un compte valide.

Les informations sensibles doivent rester secrètes : Il est également crucial d'éviter de partager des données personnelles et sensibles en ligne, telles que son adresse, des informations financières ou d'autres données d'identification personnelle. Ce sujet nécessite une attention particulière, car c'est précisément ce type d'informations qui vaut son pesant d'or pour les pirates – si un utilisateur sollicite explicitement ce genre de données, il s'agit d'un important signal d'alerte et toute communication doit être interrompue.

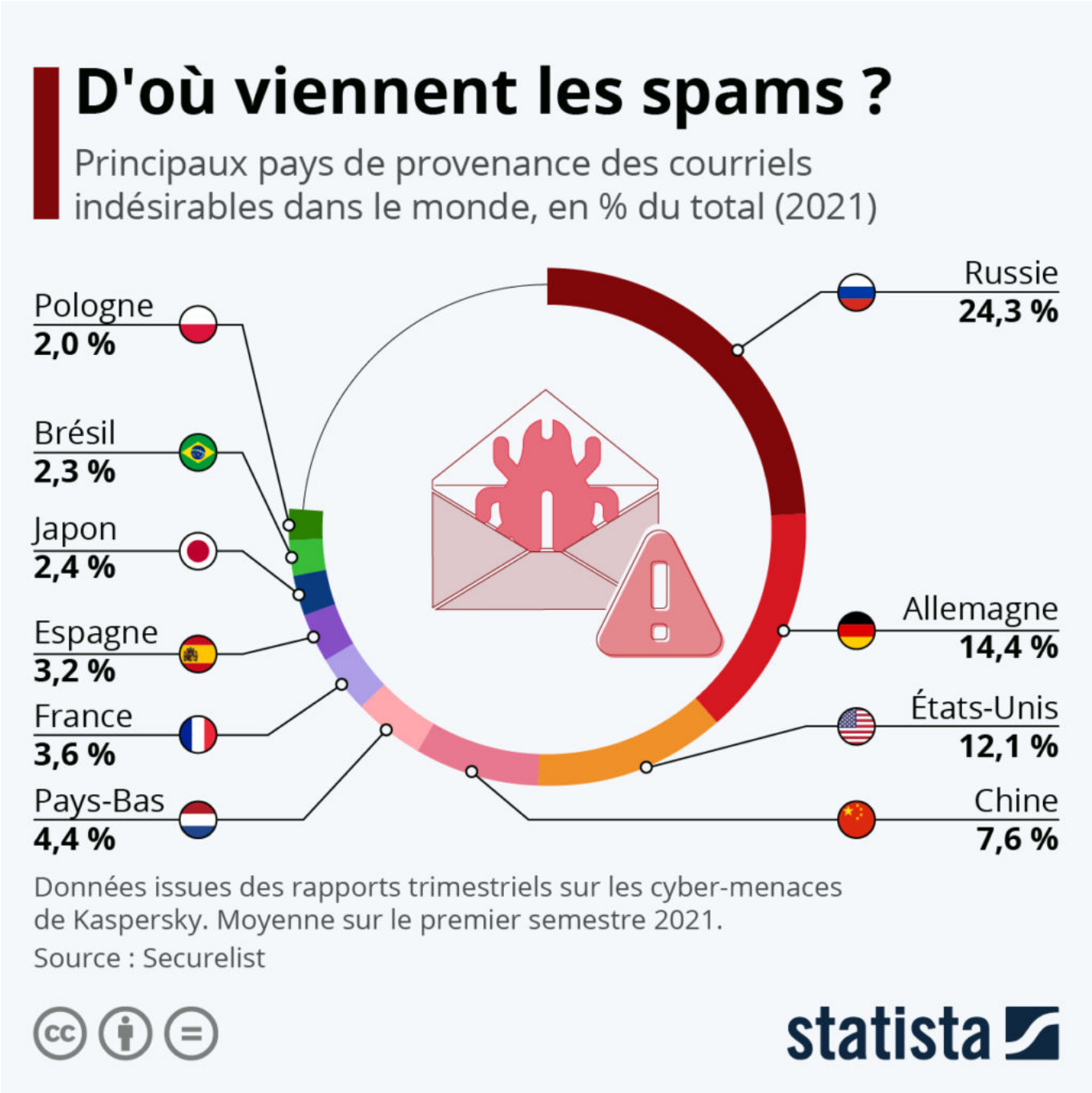
Savoir qui a accès à quoi : Dans le monde de l'entreprises si vous n'avez pas le contrôle ni la visibilité de savoir qui a accès à quoi au sein de votre système d'information …vous êtes en grand danger. Seule une solution de gestion de vos identités peut y remédier. »

« Cette année encore, la Saint Valentin promet d'être une occasion lucrative pour des cyber criminels qui exploiteront le désespoir des personnes seules, tout comme l'envie de faire plaisir des personnes en couple. Les menaces sont tout aussi importantes de part et d'autre. Toutefois, si les utilisateurs sont conscients des dangers et restent attentifs à certains points et signaux d'alerte qui révèlent de potentielles actions frauduleuses, ces attaques resteront vaines et les identités digitales seront saines et sauves. »

Les pays qui émettent le plus de spams

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025



Les spams envahissent inlassablement nos boîtes mails. Ils représentent près la moitié de la totalité des courriels envoyés dans le monde et après un déclin prolongé, leur part dans le trafic mondial de mails a recommencé à augmenter en 2021, comme le rapporte Securelist dans son dernier rapport trimestriel. Se désinscrire des listes d'e-mailing ou ne donner son adresse e-mail qu'avec parcimonie ne permettent pas de s'en protéger complètement. Et même si la plupart atterrissent directement dans les courriers

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

indésirables, ils n'en sont pas moins exaspérants et font tous les ans de nombreuses victimes, le mail restant le principal vecteur des cyberattaques.

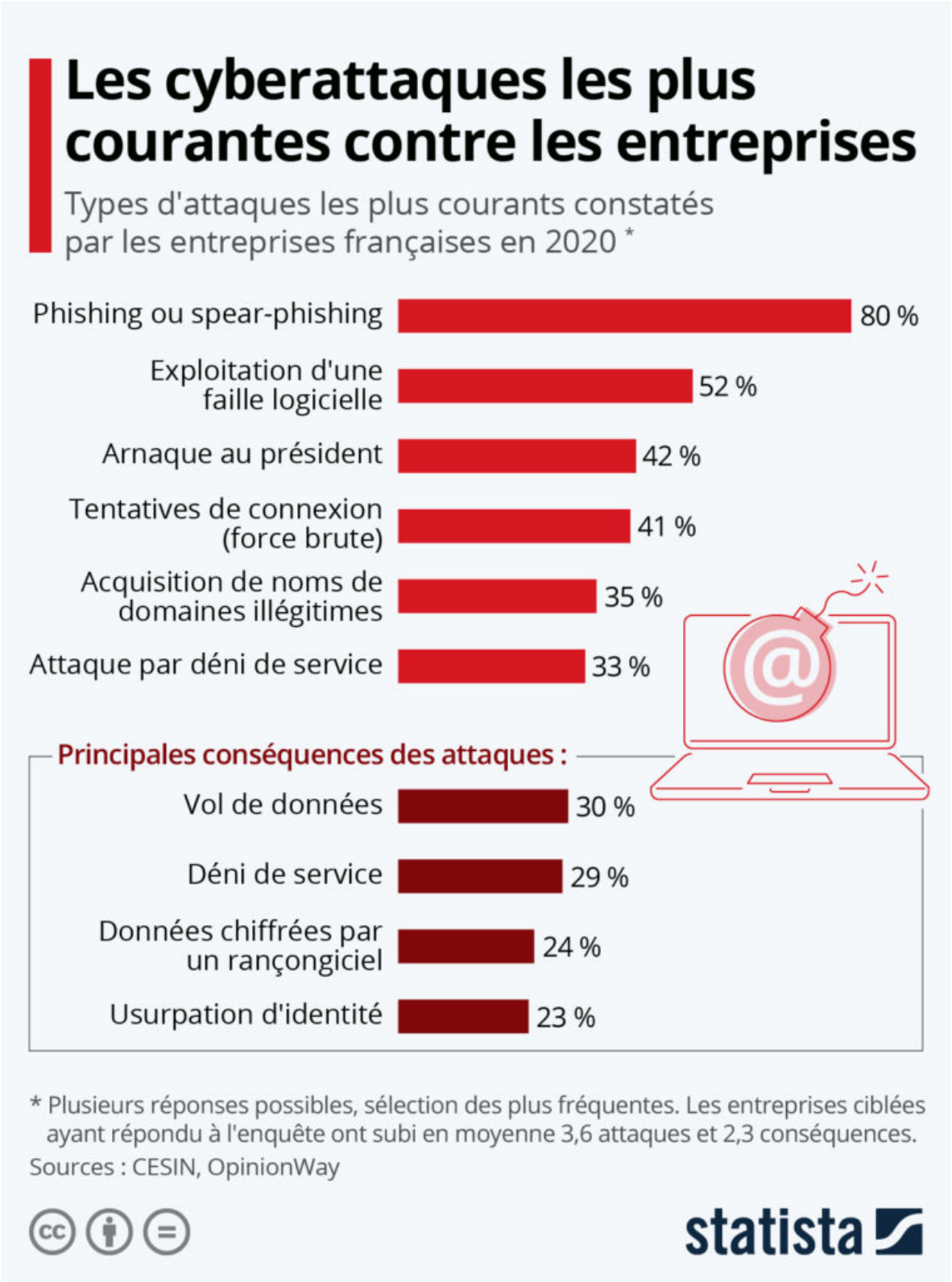
Toujours selon les données de Securelist, 76 % des spams envoyés dans le monde proviennent de dix pays. La Russie est le premier pays émetteur dans le monde : elle représentait près du quart du trafic mondial de courriels indésirables au premier semestre 2021. L'Allemagne occupe le deuxième rang (14,4 %), suivie par les États-Unis (12,1 %) et la Chine (7,6 %). Bien que seuls 3,6 % des spams mondiaux proviennent de France, cela place tout de même l'Hexagone dans les six principaux pays émetteurs juste derrière les Pays-Bas (4,4 %).

De Tristan Gaudiaut pour Statista

Les cyberattaques les plus courantes contre les entreprises françaises

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025



Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Samedi dernier, les Etats-Unis ont de nouveau été frappés par une cyberattaque massive. Des pirates informatiques ont ciblé la société américaine Kaseya, qui fournit des logiciels de gestion de réseaux, pour demander une rançon à potentiellement plus de 1 000 entreprises clientes du groupe. Les hackers ont utilisé un rançongiciel, un programme qui exploite une faille de sécurité pour paralyser un système informatique avant d'exiger une rançon pour le débloquer. L'une des conséquences a été la fermeture temporaire de 800 supermarchés en Suède, les caisses de l'enseigne ayant été mises hors service lors de l'attaque.

D'après le dernier baromètre de la cybersécurité publié par le CESIN, le vecteur d'attaques le plus courant constaté par les entreprises françaises reste le phishing ou spear-phishing, qui consiste à piéger des utilisateurs en leur envoyant un mail leur faisant croire qu'ils s'adressent à un tiers de confiance. Ce type d'attaque a été rapporté par 80 % des entreprises ciblées en 2020. Il est suivi par l'exploitation des failles logicielles, qui concerne un peu plus de la moitié des entreprises interrogées. Comme le montre également notre graphique, les principales conséquences de ces cyberattaques sont le vol de données (30 % des entreprises attaquées), le déni de service (29 %) ainsi que le chantage via un rançongiciel (24 %). Les auteurs de l'étude soulignent que la crise sanitaire a confronté les entreprises à de nouveaux cyber-risques, en lien notamment avec la généralisation du télétravail et l'usage d'applications et de services Cloud dont la sécurité fait défaut.

De Tristan Gaudiaut pour Statista

Cybersécurité : 6 précautions à prendre avant de partir en vacances

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Même durant l'été les cyber menaces ne prennent pas de vacances. Benoit Grunemwald, expert en cybersécurité chez ESET France vous propose de suivre six étapes en amont de votre départ en vacances afin de profiter de vos congés estivaux en toute sérénité.

Les vacances d'été approchent à grands pas et avec elles les cyber menaces associées. Pour partir en voyage l'esprit léger et vous offrir des congés en toute sérénité, suivez nos quelques conseils. Voici les bons gestes à adopter en amont de votre départ estival :

1. N'annoncez pas votre voyage publiquement
Il est tentant d'annoncer sa joie de partir en voyage sur les réseaux sociaux. Malheureusement, par ce biais, vous donnez alors les mêmes informations à vos amis qu'aux cyber criminels et cambrioleurs, qui peuvent donc cibler leur phishing selon votre lieu et vos dates de voyage. Faites tout autant attention à votre réponse automatique sur vos boites mails professionnelles et personnelles. Le message doit rester concis.

2. Faites des sauvegardes
Avant votre départ, sauvegardez toutes vos données sensibles pour les récupérer en cas de perte ou de vol de votre matériel informatique. Personne n'est à l'abri d'un malheureux accident. Une sauvegarde de vos données minimisera alors la perte. Vous pouvez multiplier cette protection en choisissant des supports physiques (clefs USB ou disques durs) et des supports virtuels via le Cloud et les Drives.

3. Modifiez (tous) vos mots de passe
Des mots de passe forts sont la première clef d'une sécurité optimale. Alors, en amont de vos vacances, modifiez ceux des appareils et de vos applications en y intégrant majuscules, minuscules, chiffres et

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

caractères spéciaux. Des mots de passe récents minimiseront leurs corruptions. Et évidemment, ces mots de passe doivent être différents entre les plateformes que vous utilisez. Ne faites pas l'impasse sur l'utilisation d'un gestionnaire de mots de passe.

4. Mettez à jour vos applications
Autre point de vigilance : les failles de sécurité. Pour les déjouer, pensez à faire une mise à jour de toutes vos applications avant de partir en vacances, que ce soient celles de votre téléphone, de votre ordinateur ou du système lui-même. Celles-ci sont régulièrement identifiées et corrigées par les développeurs et il est important de toujours avoir les dernières versions pour un minimum de risques.

5. Renseignez-vous
Avant chaque voyage, tâchez de connaitre les principales informations sur votre lieu de villégiature pour parer aux éventuels problèmes techniques que vous pourriez être amené à rencontrer. Votre hôtel est-il équipé d'un réseau sécurisé ? Les prises de vos chargeurs correspondent-elles ? Y a-t-il des frais pour les appels vers vos proches ? Une fois ces informations acquises, prenez des mesures en conséquence : augmentation de votre forfait téléphonique, achats d'adaptateurs, installation d'application pour des appels en Wi-Fi.

6. Installez des outils de protection
Vous emmènerez certainement en vacances vos appareils mobiles : protégez-les. Les VPN permettront de limiter votre exposition à certaines attaques en chiffrant vos communications et en empêchant ainsi les pirates de les intercepter ou de les modifier. Si vous pensez utiliser vos appareils électroniques dans des lieux publics, posez sur l'écran un filtre de confidentialité pour qu'ils deviennent illisibles pour vos voisins. Pensez aussi à vous équiper d'un matériel vous permettant d'avoir toujours votre téléphone sur vous lorsque vous pratiquerez vos activités : une coque étanche sera notamment utile pour vous baigner avec votre smartphone, et ainsi échapper à un vol éventuel sur la plage…

Benoit Grunemwald, expert en cybersécurité chez ESET France

Avignon, le système d'information n'a jamais eu autant besoin de Probe iT !

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Sabrina Feddal, ingénieure systèmes et réseaux a créé, en 2016, la société Probe it, spécialisée dans la cyber sécurité. Son équipe et elle interviennent auprès des petites et grandes entreprises pour la mise en sécurité de leur système d'information. Une expertise qui s'inscrit dans l'évaluation du risque jusqu'à la mise en place de remparts adéquats et opérants, en passant par la formation du personnel.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Travail & persévérance
«Je suis issue d'un milieu modeste et l'obtention d'un diplôme d'ingénieur Systèmes et réseaux consacrait tout le travail et la persévérance que j'avais investis, notamment lors des classes préparatoires, sourit Sabrina Feddal, la dirigeante de Probe iT. Ma carrière s'est poursuivie, en tant que salariée, durant une quinzaine d'années en tant qu'ingénieur réseaux pour venir progressivement à la sécurité et à la protection des données. Les attaques informatiques, vers les années 2 000-2010 n'étaient alors pas aussi répandues qu'aujourd'hui. Ce domaine se voulait, à l'époque, nécessaire même si aujourd'hui, il a pris beaucoup d'ampleur.»

Sécurité rime avec organisation
«J'ai abordé ce nouveau volet de la profession par le biais de la technique appelée Sécurité opérationnelle. Je réalisais l'ingénierie, c'est-à-dire l'architecture de protection. Petit à petit j'ai évolué sur l'aspect plus organisationnel car la sécurité n'est pas que l'affaire des techniciens et ingénieurs, elle touche également l'humain. Beaucoup d'attaques peuvent aboutir lorsque l'on clique sur un mail ou que l'on s'est fait piéger au téléphone. On en vient à toucher la composante des Ressources humaines puisqu'il faut former l'ensemble des collaborateurs aux bonnes pratiques et même, d'un point de vue technique, via des volets de sécurité d'accès physique. La sécurité est très transverse et nécessite de l'organisation. Peu à peu j'ai occupé des postes de conseil auprès du directeur informatique, puis de la direction générale pour les accompagner dans une démarche qualité, d'amélioration continue, notamment, sur le plan d'actions dévolues à la protection et à la prévention des attaques, faire en sorte qu'elles ne se produisent pas et si cela advenait, pouvoir y réagir dans les meilleurs délais pour rétablir une situation normale.»

La cyberattaque
«Et puis la cyberattaque s'est généralisée. A l'origine ça pouvait être l'adolescent qui essayait, par défi, d'aller hacker telle ou telle société. Ça pouvait être la concurrence, les Etats… La cyberattaque pouvait cibler les établissements de santé. Là, nous sommes plus sur des attaquants crapuleux, de la délinquance en ligne… Au fil des années, celle-ci a d'ailleurs bien compris l'intérêt d'Internet en démultipliant sa portée sur des millions de cibles, comme, par exemple, en menant une campagne de phishing (hameçonnage, récupération de données), ce qui est, proportionnellement, beaucoup plus rentable. Aujourd'hui, Internet se structure, se réglemente mais, préalablement, la délinquance s'est mondialisée au-delà des frontières françaises, ce qui induit plus de difficultés et donc le ralentissement des investigations.»

Concrètement
«Le réseau de cyber criminels appelé Emotet (Cheval de Troie bancaire) qui orchestrait, depuis plusieurs années, des attaques pour récupérer des données bancaires a été mis au jour et démantelé par Interpol, aux termes de plus de deux ans de travail acharné, en ayant noué des coopérations internationales et mobilisé plus de huit pays. Si les serveurs ont été saisis, on n'a pas entendu parler de criminels véritablement identifiés car, techniquement, Internet pose des difficultés à la traçabilité et s'appuie sur le relatif anonymat que permettent les outils informatiques. En clair ? On n'arrive pas à tracer les personnes et les groupes. Vous avez l'impression que le flux malveillant vient de tel pays, alors qu'en réalité, il provient d'un autre.»

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Les places de marché

«Un autre exemple ? Vous croyez saisir vos codes carte bleue sur un site identifié alors que vous renseignez le serveur de l'attaquant, lui permettant de se servir de votre carte bleue. Ces données sont ensuite mises en vente sur les places de marché organisées du Darknet sur Alphabet et autres… Ces places vont, en quelque sorte, professionnaliser les délinquants et leur permettre la revente de données, de bloquer l'activité d'entreprises pour les rançonner comme ça a été le cas avec les hôpitaux, ou l'Afnor (Association française de normalisation) ou encore Bouygues construction. Là, non seulement l'outil est bloqué mais en plus un chantage s'exerce à la publication de données confidentielles.»

De nouvelles initiatives

«Pourtant, des cadres réglementaires visent à plus de protection, plus de respect de la vie privée notamment avec le RGPD (Règlement général sur la protection des données) qui va consacrer la protection de la vie privée des citoyens européens. La France s'inscrit, depuis quelques années, dans la loi de programmation militaire, un enjeu national, qui identifie un certain nombre d'opérateurs vital ayant l'obligation de sécuriser leur système d'information pour éviter la catastrophe en cas de panne majeure qui pourrait impacter la vie des citoyens. Ces cadres s'organisent, imposent la sécurité aux différentes parties prenantes de la société, en tout cas pour les grands acteurs, les grands groupes. Par ruissellement, cela impactera les sous-traitants, tout comme le tissu des TPME (Très petites et moyennes entreprises) qui, indirectement, vont devoir également se conformer à ces nouvelles règles. Evidemment, le risque zéro n'existe pas, cependant le socle minimal de sécurité permet d'éviter d'être la proie facile d'attaquants comme on a pu voir les attaques se multiplier auprès des établissements de santé qui ne bénéficient peut-être pas d'assez de sécurité sur place, ce qui est peut-être aussi le cas des TPME.»

Les clients

«Nos clients ? Le milieu de l'enseignement, de la banque, de l'assurance, des mutuelles… Si nous étions, à l'origine, axés sur les grands comptes, depuis plus de cinq ans nous travaillons aux côtés des petites et moyennes entreprises dont nous comprenons les problématiques dans le sens où elles sont débordées par d'autres sujets, et particulièrement pendant cette crise sanitaire. D'ailleurs, à ce sujet, le télétravail a été le point d'entrée de pas mal d'attaques du fait qu'il n'était pas suffisamment sécurisé. Il faudra travailler à ce qu'il ne soit pas le maillon faible, le trou de sécurité et donc la porte d'entrée dans le système d'information de l'entreprise.»

Un marché ultra concurrentiel

«Nous cultivons l'expertise au quotidien, s'il y a beaucoup de concurrents il y a aussi une pénurie des ressources, alors nous misons sur la qualité de nos prestations, en termes d'expertises nous sommes certifiés en sécurité CISSP (Certified information systems security professional) ; des certifications sectorielles dans le domaine de la protection des données monétiques : cartes bancaires PCIDSS (Normes de sécurité de l'industrie des cartes de paiement), des certifications sur les bonnes pratiques, les normes, l'organisationnel Iso 27 001 (Mise en œuvre et gestion d'un système de management de la sécurité de l'information), sur l'analyse de risque qui est très demandé, Iso 27 005 (Gestion des risques en sécurité de l'information), techniquement nous travaillons avec des personnes certifiées qui permettent de faire des tests d'intrusion, ce qu'on appelle des certifications OSCP (Offensive security certified professional) avec des professionnels surentraînés en laboratoires virtuels qui passent un examen réel sur 24 à 48h

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

pour faire 'tomber' une centaine de machines. Nous nous démarquons également par l'expertise d'expérience car, comme je vous le disais, nous faisons face à une pénurie de talents et lorsque ceux-ci arrivent sur le marché, ils ne possèdent pas notre expérience.»

Le coût de la sécurité

«C'est aussi toute la problématique du coût d'un service plus que nécessaire. Nous avons identifié, chez Probe iT le fait que les PME n'ont pas de budget exponentiel au regard de leur chiffre d'affaires et aux solutions mesurées et adéquates pour assurer leur sécurité. C'est la raison pour laquelle nous proposons aussi de l'accompagnement, du conseil, pour que les réalisations techniques ne soient pas que l'apanage de cabinets parisiens ou nationaux. C'est justement sur ce créneau que nous portons notre valeur. Nous sommes un cabinet à taille humaine avec une offre de services et des solutions abordables. Nous avons développé des plateformes de sensibilisation, des offres de mise en conformité au RGPD, pareil pour l'évaluation du niveau de sécurité qui est la 1re chose à faire pour savoir si l'on est suffisamment sécurisé et ce que l'on peut faire de plus. Autant de packages à proposer à des prix raisonnables.»

Demain ?

«Nous continuons sur notre lancée, espérant conforter notre position dans le tissu économique local, plus largement national et international. Nous proposons à nos clients deux plateformes : Sensibilisation et RGPD qui vont continuer à évoluer, complétées d'un mixte services-solutions pour pouvoir répondre à la demande du marché. Nous maintenons une veille d'actualité sur la cyber sécurité et l'intelligence artificielle, plus de 1 200 personnes nous suivent depuis la création du compte parmi lesquels des influenceurs sur Twitter et veillecyber.com

Au tout début ?

«Ce qui m'a fait basculer dans l'entrepreneuriat ? Le besoin d'indépendance et de liberté par rapport au cadre salarié de l'époque, avec la vocation de revaloriser le métier d'ingénieur par rapport à la séniorité, au parcours. Dans nos métiers nous manquons de bras et de cerveaux. Alors j'enseigne dans une école d'ingénieurs pour former les jeunes générations. Cela m'a donné envie de monter une structure qui reflète mes valeurs : de l'âme, de la transmission, plus de place pour les femmes – qui ne représentent que 10 à 11% des ingénieurs- en cyber sécurité. Chez Probe iT ? Nous existons depuis 2016 et sommes 5 femmes. Ce n'est pas de la discrimination (rires) mais ça s'est fait comme çà. Mon chiffre d'affaires ? Ça reste confidentiel. Notre portefeuille clients ? Nous sommes positionnés sur de grands comptes dans le secteur bancaire, de l'assurance, des mutuelles, de la sphère médicale comme cette fondation qui compte plus de 15 établissements médicaux, cliniques de soins et de psychiatrie avec des données extrêmement sensibles sur la sécurité et au sens du RGPD. C'est la raison pour laquelle, dans mon équipe, nous accueillons des juristes pour une approche globale, cohérente car, de plus en plus, la cyber sécurité est réglementée.»

La proposition

«Nous proposons d'organiser l'amélioration continue de la sécurité, de sensibiliser les collaborateurs des entreprises ; de piloter la mise en conformité normative et réglementaire de celle-ci. L'entreprise a besoin d'établir et de maintenir la confiance numérique ; d'évaluer son niveau de sécurité ; de protéger son activité et ses données sensibles. Nous sommes experts en audit sécurité et RGPD ; nous portons

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

assistance en cas de piratage et nous assurons une assistance technique.»

Créativa
«Nous sommes ravis d'être hébergés chez Créativa, d'être chez les FCE (Femmes cheffes d'entreprise), nous faisons également partie de la French Tech, du Clusir Paca (Club de la sécurité Paca en Avignon), nous allons adhérer à la Cpme 84 (Confédération des petites et moyennes entreprises) de Vaucluse. Nous avons été accueillis à bras ouverts par les réseaux de Vaucluse. Si j'avais un conseil à donner je dirais : 'Installez-vous à Agroparc car ce sont un lieu et des associations qui dynamisent les entreprises. L'endroit est bienveillant et tout y est facilité'.»
Probe iT, hébergée chez Créativa à Agroparc. 200, rue Michel de Montaigne 84140 Avignon. 04 90 23 67 59. contact@probe-it.fr et probe-it.fr

Sabrina Feddal, ingénieure systèmes et réseaux a créé, en 2016, la société Probe it, spécialisée dans la cyber sécurité.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Vers un marché unique du numérique ?

La semaine dernière vient de se tenir à Lille le FIC (Forum International de la Cyber sécurité). Cet événement mondial de référence en matière de sécurité et de confiance numérique rassemble chaque année près de 10 000 participants. Entre- tien avec Guillaume Tissier, président de la CEIS (Compagnie européenne d'intelligence stratégique)

■ Le FIC change de dimension cette année, en passant sur trois jours au lieu de deux. Pourquoi ?

« Nous avons ressenti le besoin d'avoir une journée supplémentaire de networking dédiée aux partenaires, de plus en plus nombreux. Et comme le nombre de participants augmente d'année en année de 20% (9 700 participants en 2019, ndlr), il était important d'étaler les participations pour ne pas se sentir à l'étroit. C'est l'occasion égale- ment d'organiser davantage de 'side event' comme la Vauban Cession à la Citadelle de Lille sur le thème de la transformation numérique des opérations militaires, à laquelle nous ajoutons l'ID Forum sur les sujets de l'identité numérique, puisque le Gouvernement travaille actuellement sur une feuille de route pour lancer la future carte d'identité numérique. Ce même jour, Acteurs publics, en lien avec la Métropole européenne de Lille, animera un temps fort sur les collectivités et la responsabilité des élus en matière de cyber sécurité. »

■ Comment les maires prennent- ils conscience de cette nécessité de transformation numérique et, donc, de sécurité des données ?

« C'est plutôt inégal en fonction des communes. Les collectivités de taille importante se sont emparées du sujet depuis quelque temps déjà mais, en revanche, de nombreuses agglomérations ou communautés de communes sont encore très en retard du fait de leur transformation numérique plus récente. Et, par conséquent, la sécurité est prise en compte plus tardivement. En octobre 2019, un 'ransomware' (ndrl logiciel de rançon) a ciblé la communauté de Grand-Cognac, en Charente, qui a complétement paralysé le système informatique. Il y a un réel impact sur les administrés avec une paralysie des services puisque de nombreuses formalités administratives se font aujourd'hui sur internet. La prise de conscience des collectivités est un véritable enjeu. »

■ Prennent-elles les choses en main ?

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

« Un certain nombre de communes se sont déjà regroupées pour monter des GIP (groupements d'intérêt public) sur les questions d'informatique et les systèmes d'information. Les collectivités possèdent des données, pour certaines, assez stratégiques. Une fuite de données des administrés peut mettre la collectivité en danger. L'impact de la trans- formation numérique est bien pris en compte mais on sent que la sécurité passe après. »

■ Pourquoi ?

« Je dirai qu'il y a les bonnes et les mauvaises raisons ! Les bonnes ? Vouloir aller vite, innover pour réduire le temps de mise sur le marché mais… cela ne milite pas vraiment pour la prise en compte de la sécurité. Et les mauvaises ? Voir la sécurité uniquement comme un coût. Bien évidemment, c'en est un mais il faut pouvoir concilier expérience utilisateur et sécurité. Le coût de la sécurité ne représente que quelques pourcents du coût global d'un projet ; le sujet le mérite bien quand on voit l'impact financier que peut avoir une fuite de données et les risques pénaux qu'il engendre. »

■ Cela passe par de la pédagogie et de la sensibilisation ?

« Chaque année, les solutions de sensibilisation et d'e-learning progressent et ce sera l'un des autres sujets du FIC : améliorer la prise de conscience de l'utilisateur, notamment sur les sujets d'ingénierie sociale. Il ne faut pas oublier non plus le côté du défenseur : effectivement, l'intelligence artificielle améliore la cyber sécurité mais il y a clairement un besoin de compétences, d'analyses et d'experts. Aujourd'hui nous sommes confrontés à un vrai problème : de nombreux postes ne sont pas pourvus, sans doute parce que nous n'avons pas assez communiqué. »

> « Une fuite de données des administrés peut mettre la collectivité en danger. »

■ Vous parliez d'utilisateur, justement, on sait aujourd'hui qu'il est le premier concerné par les sujets d'authentification.

« Le sujet de cette année porte sur la place de l'humain dans la cyber sécurité car le cyber espace est avant tout un espace humain. Le sujet de la sécurité n'est pas uniquement technique ou technologique. L'utilisateur reste, et heureusement, l'Homme. L'expérience utilisateur, en termes de sécurité, a été très longtemps négligée et on a trop pensé que la sécurité ne pouvait pas être ergonomique. Il n'est plus possible d'utiliser les anciens dispositifs. Aujourd'hui, un utilisateur possède plus d'une centaine de mots de passe. Autre aspect de ce thème : la victime, qui se fait avoir en ayant été naïve ou négligente. On voit bien que le facteur humain joue dans la plupart des cas et le courriel reste le premier vecteur d'infection.

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

Il faut encore et toujours travailler sur la sensibilisation. Un 'fishing' sur quatre est ouvert par les utilisateurs : cela veut donc dire qu'il y a encore des progrès à faire ! »

■ Quelles solutions préconisez- vous pour améliorer l'authentification ? On parle de la fin des mots de passe, est-ce réellement possible ?

« On l'annonce depuis long- temps ! C'est un vrai sujet, en effet. Aujourd'hui, il existe des technologies de biométrie et de biométrie comportementale qui peuvent permettre d'apporter des solutions en termes d'authentification. Les authentifications à deux facteurs (de type 3D Secure qui envoient un message lors d'un paiement, ndlr) sont perçues comme lourdes et contraignantes par les utilisateurs. Toute la question est de trouver comment simplifier ces démarches. Pourquoi ne pas imaginer un dispositif tel que France Connect (qui permet d'accéder plus facilement aux services publics via un compte unique) ? Cela suppose de créer des écosystèmes acceptant les mêmes identifiants et identités. Mais je suis convaincu qu'adopter cette logique d'éco- système et avoir un dispositif d'authentification dont la gestion permet de se connecter à différents services est, pour l'utilisateur, une bonne solution. »

■ Peut-on s'inspirer d'autres pays sur ces sujets ?

« L'Estonie est souvent citée en exemple sur l'identité ; il y a aussi des expériences intéressantes en Belgique. En France, nous sommes malheureusement un peu en retard et c'est assez paradoxal car sur ces sujets d'identité, et notamment sur la partie du support physique de l'identité, notamment avec les cartes à puce, nous étions à la pointe il y a quelques années. Pour des tas de raisons nous avons pris du retard. Nous sommes en train de le combler. En matière de cyber sécurité, l'éco-système français est très innovant, avec de nombreuses PME qui développent des solutions localisées selon les besoins. La difficulté à laquelle nous faisons face c'est l'accélération de ces entreprises. Faute d'avoir, sur le territoire, de grands groupes ou de gros éditeurs généra- listes spécialisés dans la sécurité qui constituent des pôles d'agrégation, les PME ne grossissent pas assez vite et se vendent trop tôt à des entre- prises étrangères. »

> « Il y a clairement un besoin de compétences, d'analyses et d'experts. »

■ Quelle est la politique actuelle du Gouvernement en matière de sécurité numérique ?

« Il y a des actions sur les différents volets : d'abord avec la montée en puissance des moyens dédiés à

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

l'ANSII (Agence nationale de la sécurité des systèmes d'informartion) sur la prise en compte de la sécurité non seulement des administrations mais aussi des services vitaux. Ensuite, sur la partie militaire et ses capacités de lutte informatique défensive mais aussi offensive, où une vraie doctrine de lutte offensive a été lancée. Le ministère des Armées cherche aujourd'hui à être autonome dans sa défense sur terre en s'appuyant sur des technologies et des moyens souverains. Dans ce cadre, le ministère a lancé plusieurs projets, notamment celui de 'Cyberdéfense factory' à Rennes en octobre 2019, ouvert à tous les acteurs du domaine cyber pour faire émerger de nouvelles technologies. Au niveau interministériel, la question réside plutôt dans la nécessité de créer un lieu – à la fois lieu de formation, de business et d'accueil des start-ups – sur le modèle du campus israélien, qui a inspiré Emmanuel Macron lors d'un voyage présidentiel. C'est un projet que nous soutenons et qui est porté par Orange Cyber défense. »

■ En 2018, la mise en place du RGPD (Règlement européen pour la protection des données) a bousculé l'ensemble du tissu économique et social. Vers quelles perspectives se tourne le marché de la cyber sécurité pour les années à venir ?

« Le débat est avant tout européen, pour avoir un marché unique du numérique. Certes, nous avons déjà fait un pas important avec le RGPD. Mais d'un point de vue du business, les marchés sont encore très cloisonnés. Une start-up ou une entreprise française de cyber sécurité se tourne d'abord vers le marché américain plutôt que vers les marchés européens. Ces sujets sont souverains mais pas unique- ment, il est possible de collaborer entre acteurs européens et sur ce point, le FIC s'est donné pour objectif de participer à ce décloisonnement international. »

Propos recueillis par Amandine Pinot La Gazette Nord-Pas de Calais pour Réso Hebdo Éco reso-hebdo-eco.com

Quelques chiffres

• Marché mondial de la cyber sécurité en 2019 : 150 milliards de dollars

• Marché français : entre 4 et 6 milliards d'euros

• Premier marché européen : la Grande-Bretagne

• Au premier semestre 2019, la CNIL a enregistré en moyenne 5,7 violations par jour

Les secteurs les plus touchés : l'hébergement et la restauration (188 violations), le commerce (177), la finance (137), les sciences et techniques (132) et l'Administration publique (92)

Causes principales : malveillance (54%), cause accidentelle (26%), violations ou fuites d'origine autre ou

Les Petites Affiches de Vaucluse depuis 1839

Ecrit par le 6 novembre 2025

inconnue (20%).

Observatoire Data Breach