EXPERT • INDÉPENDANT • SANS PUBLICITÉ

QUE CHOISIR

pratique

Numéro 146 • Décembre 2025 • 7,30 €

Vos données

GARDEZ LE CONTRÔLE !

- LES DÉRIVES DE L'IA
- RÉAGIR EN CAS DE FRAUDE

Tests

35 logiciels
gratuits ou payants
pour se protéger

+ **HUILE D'OLIVE**
Nos conseils pour la choisir

L 13463 - 146 - F: 7,30 € - RD

DROM-COM : 8,50 € / 990 XPF

Consultez chaque trimestre nos

NUMÉROS PRATIQUES

7,30 € chaque numéro

Vous avez entre les mains la toute dernière édition de ***Que Choisir Pratique.*** Mais ce n'est pas la seule ! Quatre fois par an, nous publions ces hors-séries sur des thèmes aussi variés et spécifiques que **l'alimentation saine, la voiture électrique, les animaux domestiques**...

Véritables encyclopédies de la consommation, les *Que Choisir Pratique* traitent la question abordée de manière approfondie, et sous tous ses aspects. Ils vous permettent **d'étendre vos connaissances, de mieux orienter vos choix et vos actions,** tout en déjouant les pièges.

POUR COMMANDER

PAR COURRIER

Remplissez, photocopiez ou recopiez sur papier libre le bulletin ci-dessous, et envoyez-le à :

Que Choisir - Service Abonnements
45, avenue du Général-Leclerc
60643 Chantilly CEDEX

PAR INTERNET

Kiosque.quechoisir.org

ou en flashant le QR code ci-contre

Nom .....

Prénom .....

Adresse .....

.....

Code postal |_|_|_|_|_|

Ville .....

	NUMÉRO COMMANDÉ	QUANTITÉ	PRIX	TOTAL
☐142	Voiture électrique		7,30 €	
☐143	Chiens & chats - Veillez à leur bien-être		7,30 €	
☐144	Mémoire - La coacher au quotidien		7,30 €	
☐145	Labels - Optez pour les vraies garanties		7,30 €	

Participation aux frais d'expédition

Je commande 1 numéro, j'ajoute **1,50 €**	
Je commande 2 numéros ou plus, j'ajoute **2 €**	

TOTAL (commande + frais d'expédition) ☐

Je joins mon règlement par chèque à l'ordre de *Que Choisir.*

Édito

PROTÉGEZ-VOUS !

Collectivités locales, opérateurs de téléphonie mobile, hôpitaux, études notariales… nombreuses sont les structures touchées par les cyberattaques. L'année 2025 a ainsi été marquée par plusieurs assauts informatiques d'ampleur, comme le révèle une étude du site Cybernews. La France apparaît particulièrement touchée, avec 1,8 million de comptes hackés entre janvier et juillet dernier. L'Hexagone prend ainsi la deuxième place des pays les plus frappés par le piratage dans le monde, après les États-Unis, qui atteignent 2,5 millions de comptes compromis. Les fraudeurs semblent toujours plus organisés et mieux armés. Les offensives – diffusion de logiciels malveillants, captures massives de données… – se multiplient et plongent les nombreuses victimes dans des situations dramatiques. Le mode opératoire est rodé: copier les données sensibles, bloquer le système, exiger une rançon de plusieurs millions d'euros. Et, si la cible refuse de payer, revendre les informations à d'autres escrocs ou les exposer publiquement. Qu'il s'agisse de données médicales, de coordonnées bancaires, de comptes de réseaux sociaux ou de documents administratifs, tout se vole et tout se revend dans un monde qui se numérise à vitesse grand V. La menace est globale et permanente… mais la riposte existe ! Des outils techniques, des lois renforcées et des gestes simples à adopter sont là pour nous protéger. Les autorités, elles aussi, montent en puissance, même si la partie reste serrée face à des gangs de plus en plus chevronnés. *Que Choisir Pratique* vous livre les clés pour reprendre le contrôle sur vos données personnelles.

Pascale Barlet

QUE CHOISIR pratique
EXPERT · INDÉPENDANT · SANS PUBLICITÉ

UNION FÉDÉRALE DES CONSOMMATEURS – QUE CHOISIR
Association à but non lucratif - 233, boulevard Voltaire - 75555 Paris CEDEX 11 - Tél. : 01 43 48 55 48

Quechoisir.org

Service abonnements : 01 55 56 71 09

Tarifs : 1 an, soit 11 numéros : 49 € ▪ 1 an + 4 hors-séries : 67 €
1 an + 4 hors-séries + 4 numéros *Que Choisir Pratique* : 94 €

PRÉSIDENTE ET DIRECTRICE DES PUBLICATIONS
Marie-Amandine Stévenin

DIRECTEUR GÉNÉRAL DÉLÉGUÉ
Jérôme Franck

RÉDACTRICE EN CHEF
Pascale Barlet

SECRÉTAIRE GÉNÉRAL DE LA RÉDACTION
Laurent Suchowiecki

CONCEPTION GRAPHIQUE
Les 5 sur 5

DIRECTEUR ARTISTIQUE
Ludovic Wyart

RÉDACTION
Damien Bancal (fondateur de Zataz.com), Camille Gruhier (cheffe de rubrique tests)

SECRÉTAIRES DE RÉDACTION
Valérie Barrès-Jacobs, Marie Bourdellès, Gaëlle Desportes-Maillet

RÉDACTRICES-GRAPHISTES
Sandrine Barbier, Clotilde Gadesaude, Capucine Ragot

INFOGRAPHISTES
David Barreto, Carla Félix-Dejeufosse, Laurent Lammens

ICONOGRAPHIE
Catherine Métayer

ODLC
Grégory Caret (directeur)

ESSAIS COMPARATIFS
Éric Bonneff (directeur), Vincent Erpelding, Neil McPherson

ASSISTANTE DE LA RÉDACTION
Fadila Benni-Nawjeek

DOCUMENTATION
Frédérique Vidal (responsable), Véronique Le Verge, Stéphanie Renaudin

MARKETING/DIVERSIFICATION
Laurence Rossilhol (directrice), Delphine Blanc-Rouchosse, Justine Boduch, Jean-Louis Bourghol, Marie-Noëlle Decaulne, Jean-Philippe Machanovitch, Francine Manguelle, Steven Phommarinh, Ibrahim Sissoko, Agathe Vaillant

JURIDIQUE
Magali Buttard (responsable), Brune Blanc-Durand, Gwenaëlle Le Jeune, Véronique Louis-Arcène, Chloé Magne

INSPECTION DES VENTES/ RÉASSORTS MP Conseil

IMPRESSION / COUVERTURE
BLG Toul, 2780, route de Villey-St-Étienne 54200 TOUL

DISTRIBUTION MLP

COMMISSION PARITAIRE
n° 0727 G82318

Imprimé sur papier Perlen Value (Suisse)

ISSN 2646-9189.

Taux de fibres recyclées : 57 %
Certification : Écolabel FSC PEFC
Eutrophisation : 620 kg CO_2/T papier

Photos de couv. : EYEM MOBILE ; SASINPARAKSA/ISTOCK

Sommaire

IMAGEFLOW/ADOBE STOCK

Les obligations légales

Sous l'impulsion de l'Europe, le paysage juridique du Web français connaît un bouleversement majeur depuis 2024. L'intelligence artificielle est désormais encadrée, plateformes et sites sont soumis à plus de transparence, et la cybersécurité devient une obligation légale pour tous les acteurs. L'identité numérique européenne prend forme… Toutefois, de nouvelles protections s'imposent vis-à-vis des mineurs et contre la fraude en ligne. Avec ce chapitre, vous saurez ce qui change en 2026 et au-delà. Sécuriser vos données personnelles est devenu impératif tant les risques sont nombreux. Pas de panique, cependant: il existe plusieurs moyens de se défendre.

EXENTIA ; ICEDMOCHA ; ALBACHIARAA/ADOBE STOCK

SOMMAIRE

Europe LA SOUVERAINETÉ NUMÉRIQUE EN MARCHE

Le Règlement général sur la protection des données, communément appelé RGPD, s'applique dans les 27 États membres de l'Union européenne. Son non-respect a coûté cher à certains !

Conçu pour garantir les libertés et les droits fondamentaux des citoyens européens vis-à-vis de leurs informations à caractère personnel, le Règlement général sur la protection des données (RGPD) découle d'une directive adoptée en 1995. Pas moins de 23 années de cheminement et d'avancées progressives ont été nécessaires avant d'aboutir à la version définitive, entrée en application le 25 mai 2018. Aujourd'hui, le RGPD intensifie la responsabilisation et l'obligation de transparence des organisations en charge du traitement de ce type de données. Il accroît aussi les droits des individus concernés. Les entreprises qui collectent, utilisent ou stockent ces éléments voient leurs devoirs renforcés: il leur est désormais imposé d'obtenir un consentement d'exploitation; de garantir le droit d'accès, d'effacement et de portabilité; de notifier les violations de données.

Tous les professionnels qui traitent des données personnelles de résidents de l'Union européenne sont soumis au RGPD.

OLEKAT/ISTOCK

DES SANCTIONS PARFOIS SÉVÈRES

Si une société enfreint ces mesures, elle risque une amende pouvant atteindre 20 millions d'euros, ou 4% de son chiffre d'affaires mondial annuel. Parmi les pénalités les plus élevées, celle de Meta (maison mère de Facebook, WhatsApp et Instagram), condamnée en mai 2023 par la Data Protection Commission (DPC) irlandaise à payer 1,2 milliard d'euros pour transferts illégaux de données personnelles vers les États-Unis[1]. Deux ans plus tard, l'Irlande infligeait à TikTok 530 millions d'euros d'amende pour transferts illicites de données vers la Chine et manque de transparence[2]. D'ailleurs, selon les sites GPDR Enforcement Tracker[3] et GDPR Fines[4], qui référencent toutes les amendes liées au non-respect du RGPD, l'Irlande détient un record en la matière (35), pour un montant réclamé de 4 milliards d'euros. En France, en septembre 2025, la Commission nationale de l'informatique et des libertés (Cnil) sanctionnait Google et Shein (le géant chinois de l'*ultra-fast fashion*) à respectivement 325 millions d'euros et 150 millions d'euros d'amendes, notamment pour *«prospection sans consentement»*[5]. ■

(1) Edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en. (2) Dataprotection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tiktok-eu530-million-and-orders-corrective-measures-following. (3) Enforcementtracker.com. (4) Gdpr-fines.inplp.com. (5) Cnil.fr/fr/tag/Sanctions.

LES FONDEMENTS DU RGPD

Ce texte aura fait couler beaucoup d'encre avant son entrée en vigueur. Le plus compliqué : garantir un traitement éthique et transparent des données personnelles des citoyens européens.

STOCKWERK/ADOBE STOCK

Le Règlement général sur la protection des données (RGPD) repose sur deux principes: chaque individu a droit à la protection de ses informations personnelles, et toute entreprise, administration ou association, quelles que soient sa taille et son activité, a la responsabilité d'assurer cette protection. Le texte définit les contours légaux de la collecte, du stockage et du traitement de ces données, et fixe un cadre juridique en matière de transparence, de confidentialité et de notification en cas de violation de leur sécurité. Les acteurs publics ou privés sont contraints de s'adapter aux exigences du RGPD afin de garantir les droits des personnes physiques se trouvant dans l'Union européenne, notamment celui «à l'oubli» (lire aussi p. 15): tout un chacun est censé avoir la possibilité de demander à n'importe quelle structure de faire disparaître de son référencement une information erronée, fausse ou malveillante le concernant.

PRÉCEPTES À SUIVRE

Qu'il s'agisse d'un moteur de recherche ou d'un webmarchand, les sociétés comme les organisations doivent être capables de fournir tous les renseignements qu'elles possèdent sur quelqu'un afin qu'ils soient modifiés, effacés ou récupérés par d'autres entités. Il leur faut avoir adopté des politiques et des procédures adéquates, formé leur personnel et renforcé la sécurisation de leurs dispositifs. Voici leurs obligations, point par point:

> **Collecte et traitement** Sociétés, administrations et associations sont contraintes de notifier aux particuliers la collecte et le traitement de leurs données personnelles, mais aussi d'obtenir leur consentement en ce sens. Ces informations ne sont censées être récoltées que si c'est vraiment nécessaire, et traitées uniquement à des fins spécifiques et légitimes.

> **Protection** Ces structures sont tenues de mettre en place des mesures techniques et organisationnelles appropriées, afin de garantir la confidentialité et la sécurité des datas. Citons l'anonymisation, le chiffrement des informations (illisibles sans une clé d'autorisation), la gestion des accès ou encore la destruction.

> **Transparence** Ces entités doivent faire preuve d'une totale transparence sur la manière dont elles traitent les données. Cela passe par la tenue d'un registre dédié (lire l'encadré ci-dessus) et par la désignation d'un délégué à la protection des données (DPO) à contacter. Celles ne respectant pas ces exigences risquent des amendes élevées, jusqu'à 20 millions d'euros ou 4% de leur chiffre d'affaires mondial (lire également p. 8). ■

UN REGISTRE, POUR QUOI FAIRE ?

Dans le but de se conformer au RGPD, les entreprises doivent créer un registre – sous forme de fichier numérique, par exemple – contenant, outre les informations personnelles (identités, adresses…), des renseignements tels que les coordonnées du délégué à la protection des données (DPO), les finalités de leur récolte (concours, abonnement…), le délai prévu pour leur effacement ou encore la description des mesures mises en place afin de les sécuriser.

Règles LES GÉANTS DU WEB PROGRESSENT

La notion de protection des données personnelles a pris de l'importance au fur et à mesure de l'essor de l'informatique puis d'Internet. Aujourd'hui, les acteurs du Web sont particulièrement surveillés.

Par «données personnelles», on entend toute information concernant une personne physique identifiée ou identifiable, comme son nom, son adresse ou son numéro de téléphone. L'expression en elle-même apparaît en 1949, quand le Conseil de l'Europe envisage pour la première fois de protéger la vie privée des citoyens des États membres. L'usage, lors de la Seconde Guerre mondiale, d'informations relatives à des individus par des militaires ou des politiques – la constitution de listes de Juifs par les nazis, notamment – a montré la nécessité d'un cadre juridique dans ce domaine. Dans les années 1970, le développement des technologies de l'information et de la communication accélère les travaux sur le sujet. À l'époque, gouvernements et entreprises commencent à collecter et stocker de grandes quantités de données personnelles, alors qu'il n'existe pas encore de réglementation en la matière et que les gens concernés ne sont pas conscients de leurs droits. Aujourd'hui, protéger la vie privée des citoyens est devenu une priorité mondiale.

UN TEXTE TRÈS STRICT

Dans l'Union européenne (UE), tout commence en 1995 avec la directive 95/46/CE sur la protection des données personnelles, remplacée le 25 mai 2018 par le Règlement général sur la protection des données (RGPD), considéré comme l'un des textes les plus stricts au monde. Désormais, les autorités des États membres sanctionnent régulièrement les entreprises qui enfreignent ces règles,

TRANSFERTS DE DONNÉES PERSONNELLES AUX ÉTATS-UNIS

Aux États-Unis, pas de loi nationale type RGPD. Chaque État fixe ses règles, de la Californie, pionnière en la matière, au Texas, plus récemment. Si les domaines de la santé, de la biométrie (ADN, empreintes digitales, etc.) et de l'intelligence artificielle font l'objet de textes ciblés, la gestion des informations personnelles s'avère parcellaire. Côté clouds (serveurs proposant des services via Internet), un accord avec l'Europe, l'EU-US Data Privacy Framework (DPF), apaise les transferts de données transatlantiques depuis juillet 2023. Mais il reste contesté quant à la protection réelle qu'il apporte… En outre, l'administration Trump a sérieusement entamé la stabilité du cadre institutionnel, ce qui jette une ombre sur sa pérennité. Le 27 janvier 2025, le gouvernement américain écartait en effet trois membres démocrates du Privacy and Civil Liberties Oversight Board, n'en laissant qu'un seul. Privée de moyens, cette instance ne peut plus superviser le mécanisme de recours, le Data Protection Review Court, élément clé du DPF. Une telle paralysie ravive, côté Europe, le risque d'une invalidation par la Cour de justice de l'Union européenne. Bruxelles et plusieurs experts conseillent déjà aux entreprises de prévoir des solutions alternatives pour leurs transferts de données transatlantiques.

GGUY/ADOBE STOCK

Google, Apple, Facebook, Amazon, et Microsoft, appelés les Gafam, enfreignent régulièrement le RGPD.

notamment les géants du numérique que sont Google, Apple, Facebook, Amazon et Microsoft (les Gafam). Le site Enforcementtracker.com permet de suivre l'évolution des actions partout dans l'Union. En France, par exemple, en septembre 2025, la Commission nationale de l'informatique et des libertés (Cnil) a infligé à Google une amende de 325 millions d'euros. Déjà, en décembre 2021, elle l'avait condamné à hauteur de 90 millions d'euros; en 2022, Bing (Microsoft) avait dû payer 60 millions; en 2023, Amazon France, 32 millions… Motifs: avoir déposé des cookies publicitaires sur les appareils de particuliers sans leur consentement et, pour Microsoft, avoir rendu plus complexe leur refus que leur acceptation. Il est, en outre, reproché à Amazon d'avoir effectué une surveillance numérique de ses employés.

En 2019, l'UFC-Que Choisir avait obtenu la condamnation de Google par le tribunal de grande instance de Paris pour 209 clauses abusives et illicites intégrées à ses conditions d'utilisation et sa politique de confidentialité. Depuis, les amendes ont atteint des montants record: en 2023, les autorités irlandaises ont sanctionné Meta à hauteur de 1,2 milliard d'euros pour transferts illégaux de données vers les États-Unis; en 2025, au Luxembourg, Amazon Europe a été condamné à payer 746 millions; TikTok a écopé de 530 millions en Irlande, et Vodafone de 45 millions en Allemagne. Cela illustre la fermeté croissante des régulateurs européens face aux géants du numérique. L'arrivée de la directive européenne NIS 2 (lire l'encadré ci-dessus) doit encore renforcer les mesures de protection et les sanctions en cas de non-respect du RGPD.

Si la notion de données personnelles évolue au fil des années, c'est aussi au fur et à mesure des avancées technologiques permettant l'usage, l'échange ou la récupération d'informations de plus en plus variées et sensibles. Il est donc capital de surveiller ces développements (intelligence artificielle, apprentissage automatique…) afin d'adapter la réglementation et de protéger au mieux les individus. ■

NIS 1 ET 2, LES BOUCLIERS NUMÉRIQUES DE L'EUROPE

La directive européenne sur la sécurité des réseaux et de l'information, ou NIS 1, date de 2016. Elle visait à protéger les secteurs critiques (énergie, finance…) en imposant à chaque pays un plan de cybersécurité. Son application, inégale selon les États, a conduit à sa mise à jour six ans plus tard: NIS 2 est en vigueur depuis 2023. Mais l'explosion des attaques et les failles numériques ont obligé à élargir la liste des secteurs protégés, à harmoniser les règles, à durcir les sanctions et à imposer une réaction rapide aux incidents. Or, cela prend du temps. La transposition de la directive a démarré par une phase de préparation du projet de loi, qui a été présenté en Conseil des ministres le 15 octobre 2024 et déposé au Parlement en vue de son adoption prochainement.

Intelligence artificielle
QUELLES DÉRIVES ?

Une requête vocale, une demande d'itinéraire et, derrière l'écran, l'intelligence artificielle commence déjà à exploiter vos données. D'ici à cinq ans, l'IA pèsera davantage encore sur notre quotidien.

Le déploiement accéléré de l'intelligence artificielle (IA) transforme la collecte et l'usage des données personnelles. Santé, éducation, justice, mobilité, objets connectés… partout, les systèmes récoltent des informations sensibles et tirent des conclusions parfois intrusives. C'est ainsi que les banques analysent désormais les appels pour détecter le «sentiment» du client et assister les conseillers en temps réel: l'IA de la Fifth Third Bank, par exemple, décrypte les voix et leur fournit des indices de tonalité et de frustration…

RISQUES PRINCIPAUX

Le danger ne vient pas seulement du progrès technique, mais également des modèles économiques des plateformes, de la capacité des entreprises à s'organiser et du respect réel des règles. D'ici à 2030, l'enjeu central sera la confiance – vérifiable, bâtie sur des moyens de protection, des contrôles externes et des règles claires.

Première menace, l'aspiration massive des données. Les modèles d'IA à grande échelle s'alimentent à des sources hétérogènes, comportant à la fois des informations publiques, semi-privées et sensibles. Des éléments concernant la santé, la biométrie, les opinions, les structures familiales, etc. se retrouvent dans des ensembles mal gouvernés et insuffisamment encadrés. Même anonymisées, les données redeviennent identifiables par croisement, déduction, reconstruction faciale, corrélation de trajectoires ou encore reconnaissance d'appartenance à un jeu de données «d'entraînement», c'est-à-dire à un ensemble d'exemples fournis à l'IA pour lui apprendre à faire des prédictions ou à prendre des décisions. C'est ainsi que les attaques par «inférence d'appartenance» (membership inference) se multiplient, démontrant qu'en acquérant des connaissances sur les données utilisées pour la production d'un modèle d'IA, un malfrat est en mesure de déduire des informations concernant une personne précise (par exemple, déterminer si elle est atteinte d'une pathologie). Et c'est aussi comme ça, si l'on revient à notre exemple bancaire, que l'IA arrive à calculer, quand un client appelle sa banque, le *churn risk* (la probabilité qu'il la quitte bientôt) à partir de signaux récents.

Deuxième risque, l'opacité. L'IA apprenant des données qu'on lui fournit, si ces dernières sont biaisées, elle reproduira et amplifiera les erreurs. Illustration: aux États-Unis, une IA dédiée au dépistage des cancers de la peau détectait moins de lésions sur les peaux

L'IA collecte, stocke et analyse des quantités massives de données personnelles pour s'entraîner.

foncées que sur les peaux claires. En cause ? Un jeu d'entraînement déséquilibré, basé surtout sur des photos de peaux claires, découvert par des chercheurs américains… Dans les domaines sensibles, il faut donc exiger des explications claires, vérifiables et contrôlables sur le fonctionnement de l'intelligence artificielle, encore trop souvent opaque.

Troisième problème, les fuites et les extractions. Une configuration du cloud erronée, un accès interne aux données abusif ou une revente suffisent. Les modèles d'IA peuvent mémoriser des fragments; avec des requêtes ciblées, noms, e-mails ou extraits réapparaissent. En septembre 2023, par erreur, des ingénieurs de chez Microsoft avaient laissé accessibles, sur Internet, 38 téraoctets (To) d'informations sensibles via un lien cloud mal configuré. L'équivalent d'un *Que Choisir Pratique* de 76 millions de pages !

Dernier angle mort, le consentement. Par défaut, vos contenus servent souvent à entraîner des IA. L'information concernant cet aspect est illisible. Le Règlement général sur la protection des données (RGPD), en Europe, et l'AI Act, aux États-Unis, fixent le cadre, mais tout dépend de la clarté des notices, de la précision des finalités et de la réalité des contrôles. La Commission nationale de l'informatique et des libertés française (Cnil) exige un exercice des droits compréhensible et intégré dès la conception; vérifiez que c'est bien le cas avant d'utiliser un service. ■

BLACKDOVFX/ISTOCK

4 GESTES POUR LIMITER L'UTILISATION DE SES DONNÉES PAR L'IA

1 **Stopper l'entraînement sur ses applications** Sur chaque appli/assistant, trouvez l'option « Confidentialité » et cherchez la ligne affichant *« Ne pas utiliser mes données pour entraîner l'IA »*. Faites-le aussi sur vos réseaux sociaux et les moteurs de recherche. Limitez les permissions d'ouvrir le micro, la caméra, les contacts et les photos en sélectionnant « Uniquement pendant l'usage » ou « Jamais ». Désinstallez ce que vous n'utilisez pas.

2 **Effacer l'historique** Videz les conversations d'IA : vos recherches, vos positions et les commandes vocales. Interdisez la collecte et programmez l'effacement automatique quand c'est possible. Désactivez les sauvegardes et les synchronisations non essentielles. Éliminez les anciennes copies dans le cloud et chiffrez celles que vous gardez. Bloquez la traque via votre navigateur : cookies tiers en « off », suppression de vos visites, demande à la fermeture et bloqueur de traqueurs.

3 **Écrire sobrement ses prompts** Ne fournissez jamais d'adresses, d'identifiants, de dossiers médicaux, bancaires, professionnels, de photos intimes, de numéros (téléphone, bancaire, assurance, etc.). Préférez des exemples fictifs. Optez pour le local lorsque vous le pouvez ; les outils hors ligne ou open source sur vos appareils peuvent être une solution. Moins de transferts = moins de risques.

4 **Exercer ses droits** Cherchez, dans toutes vos applications, les « Données personnelles ». Trouvez « Accès/effacement/opposition » et demandez à recevoir ce que la société connaît de vous. N'hésitez jamais à en réclamer la destruction et la preuve de celle-ci, via ce type de message : *« Je m'oppose à l'usage de mes données pour l'entraînement d'IA. Merci de confirmer. »* Pour finir, passez en revue tous les trois mois vos applications, leurs permissions, historiques, sauvegardes et paramètres d'entraînement.

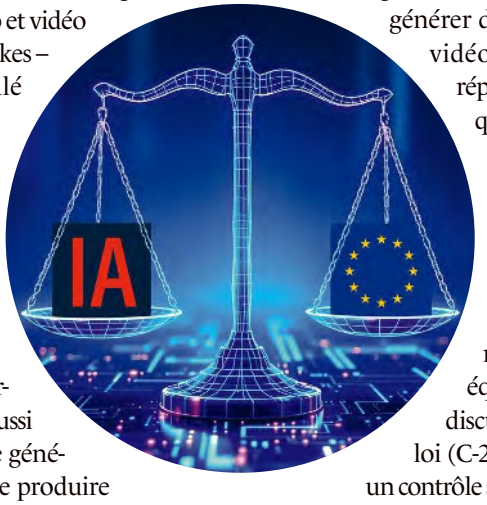
AI Act L'UE MUSCLE LA PROTECTION DES CITOYENS

Face à l'essor fulgurant de l'intelligence artificielle, l'Union européenne a conçu un cadre normatif clair. Ce règlement – l'AI Act –, entré en vigueur le 1er août 2024, pose ses conditions.

Plusieurs contraintes s'appliquent au Web européen depuis février 2025. Certains usages de l'intelligence artificielle (IA) jugés dangereux ont été interdits, comme la reconnaissance faciale de masse et le «scoring social». Cette dernière pratique consiste à collecter les informations concernant un individu (achats, localisation, recherches sur Internet, habitudes de paiement, etc.) puis à lui attribuer, via un algorithme, une note censée refléter son comportement, son profil ou un risque. Par ailleurs, n'importe quel contenu sur la Toile qui a été généré ou modifié par IA – notamment les images et les enregistrements audio et vidéo «hypertruqués», ou deepfakes – doit dorénavant être signalé aux internautes.

TRAÇABILITÉ ET CONTRÔLES

Les réseaux sociaux ont déjà tous intégré un message d'alerte à ce sujet dès qu'une image ou une vidéo est diffusée. Depuis août dernier, les règles s'appliquent aussi aux modèles d'IA «à usage général» (c'est-à-dire capables de produire du texte, des images ou du code), avec de nouvelles obligations de gouvernance, de sécurité et de transparence. D'ici à 2026-2027, les secteurs dits à haut risque (santé, justice, éducation, emploi…) devront aussi se conformer à des normes strictes de traçabilité et de contrôle des biais. Ces mesures complètent le RGPD, qui protège les données personnelles en encadrant les droits d'accès, d'opposition, de suppression ainsi que le profilage. À présent, un utilisateur peut non seulement demander la suppression des informations le concernant, mais encore obtenir des explications claires sur l'utilisation de celles qu'il donne par un système d'IA. Cette vigilance répond à des menaces bien réelles: arnaques à l'usurpation d'identité, désinformation virale, deepfakes trompeurs…



CUTEBEE/ADOBE STOCK

DEUX OBLIGATIONS

Pour les contrer et authentifier les contenus, l'Union impose deux éléments aux concepteurs d'IA générative (ces systèmes capables de générer du texte, des images et des vidéos ou d'autres médias en réponse à des requêtes): le marquage numérique (ou *watermarking*, lire également le lexique p. 111) et les métadonnées sécurisées.

Ailleurs dans le monde, la situation varie. Alors que les États-Unis n'ont pas de réglementations fédérales équivalentes et que le Canada discute encore de son projet de loi (C-27), la Chine applique déjà un contrôle strict de l'IA générative. Une chose est sûre, la course entre l'IA et la régulation ne fait que commencer. Le travail restant à réaliser est immense, comme en témoignent certains faits. Ainsi, avant que la possibilité ne soit bloquée, les moteurs de recherche Bing, DuckDuckGo et Google remontaient encore, en août 2025, des documents ayant été générés par ChatGPT, d'OpenAI, et Grok, de X (ex-Twitter). ■

UN VRAI DROIT À L'OUBLI

Vous souhaitez reprendre le contrôle de vos données personnelles ? Voici la marche à suivre, en cinq points.

Si un site ou un moteur de recherche ont sauvegardé vos données sans votre consentement, n'hésitez pas à contacter la Cnil, qui vous aidera.

Déterminer ce qu'Internet sait de vous débute par cette question: votre adresse électronique a-t-elle été sauvegardée quelque part dans un espace numérique (sites, blogs…)? Si vous voulez le savoir, demandez à un moteur de recherche (Google, par exemple) de détecter tous les fichiers texte référencés dans ses bases de données. Pour cela, tapez le code suivant dans le cadre de recherche: «inurl:.txt». Cette commande, ou *dork,* peut se «traduire» de la sorte en français: «Google, peux-tu trouver, dans toutes les URL (adresses web) que tu as en mémoire, celles finissant par .txt?» Cette requête est néanmoins un peu trop large, car le moteur affichera alors toutes les plateformes qui proposent un document en .txt – les réponses ne seront donc pas précises. Afin d'affiner les résultats, ajoutez à votre demande l'objet sur lequel porte la vérification – soit, ici, votre adresse mail. Le *dork* s'écrit alors ainsi: «inurl:.txt votre@mail.fr» (rappelons qu'il est possible de remplacer cette adresse mail par n'importe quel autre intitulé ou type de fichier, Word, PDF…). À savoir: les pirates utilisent également cette technique pour faire ressortir les identifiants de connexion et les adresses électroniques enregistrés dans les serveurs des sites internet…

1 CONTACTEZ LES ADMINISTRATEURS

Une fois que vous avez repéré tous les sites qui stockent votre adresse électronique sans votre accord, il faut contacter leurs administrateurs, en espérant qu'ils vous répondent (ou que vous ne faites pas face à des blogs abandonnés, par exemple). Une erreur commise doit impérativement pouvoir être corrigée ! Premier point: leur rappeler les obligations du RGPD, c'est-à-dire avertir la Commission nationale de l'informatique et des libertés (Cnil), régler le problème et agir de manière qu'il ne se reproduise plus. Ils sont, en outre, tenus d'alerter toutes les personnes impactées en cas de fuite des données.

2 SOLLICITEZ LA CNIL

Gardez une copie de vos démarches. En cas de refus d'obtempérer, de silence des moteurs de recherche ou de webmasters ayant sauvegardé vos données sans votre consentement, n'hésitez pas à faire appel à la Cnil, qui vous aidera. Légalement, un moteur de recherche dispose de trois mois au maximum pour agir et vous répondre. La norme est d'un mois. Si le délai se prolonge, le responsable du traitement des données doit vous prévenir et motiver le retard. Vous avez essuyé >>

>> un rejet? La Cnil propose un formulaire de plainte[1]. Le processus se poursuivra jusqu'à la mise en place effective du droit à l'oubli.

3 FAITES JOUER LA LOI

Qu'elles se nomment Google, Bing (Microsoft), Yahoo !, Archive, YouTube ou encore Qwant, ces plateformes mondiales ne peuvent pas faire tout ce qu'elles veulent. Fort heureusement, la loi est du côté des internautes. Depuis 2014, la Cour de justice de l'Union européenne a renforcé la protection de ses citoyens face à la diffusion de leurs informations personnelles par les moteurs de recherche. Ainsi, ils ont le droit de leur demander d'effacer les résultats qui comportent leur nom (lire lettre ci-dessous) si ces derniers sont «*inappropriés, inexacts, périmés, non pertinents ou excessifs*». Les acteurs du référencement disposent d'un mois pour répondre. Attention, quand le renvoi sur le lien incriminé disparaît d'un moteur, le document en lui-même (ou la page) est encore accessible sur Internet (lire ci-dessous).

4 SUPPRIMEZ DÉFINITIVEMENT VOS DONNÉES

Si activer le droit à l'oubli sur les moteurs de recherche est aujourd'hui normé et contrôlé par la Cnil[2], retirer un lien vers un contenu ne suffit pas à la suppression effective de ce dernier. Pour qu'il soit réellement éliminé et ne réapparaisse pas dans de nouveaux référencements, il faut contacter directement l'administrateur du site en question. Un courriel est, certes, plus rapide, mais mieux vaut lui envoyer un courrier postal en recommandé (lettre type ci-dessous).

5 VÉRIFIEZ SUR ARCHIVE.ORG

Internet Archive est un projet gratuit et ouvert à tous, depuis 1996, dont l'objectif est de préserver le patrimoine culturel et historique d'Internet. Cette sorte de bibliothèque numérique récupère, indexe, stocke et rend accessible des milliards de pages web sur Archive.org. Baptisée aussi Wayback Machine («machine à retourner en arrière»), elle regroupe tous types de supports tels que des logiciels, des images, des livres, des fichiers audio, des vidéos… Des informations personnelles erronées pouvant y être enregistrées, envoyez un courriel à info@archive.org afin de les faire effacer, en indiquant l'adresse URL du domaine litigieux et la raison pour laquelle vous désirez que la sauvegarde soit supprimée. Dans certains cas, on peut vous demander de confirmer la propriété du site référencé et stocké sur Wayback Machine; il vous faudra alors faire appel à son webmaster. ■

(1) Cnil.fr/fr/plaintes. (2) Cnil.fr/fr/comprendre-mes-droits/droit-au-dereferencement.

À adresser à un administrateur de site pour se faire déréférencer. Toute personne peut invoquer son droit à l'oubli.

Madame, Monsieur,

Des informations me concernant sont actuellement diffusées sur votre site internet, sur les pages suivantes : **[adresse_du_site_web].**

Aussi, en application des articles 21.1 et 17.1.c. du Règlement général sur la protection des données (RGPD), je vous remercie de supprimer les données personnelles suivantes me concernant : **[infos_à_supprimer]**.

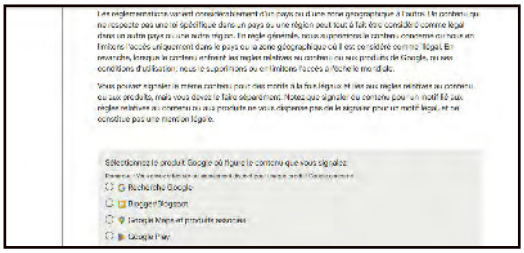
Je souhaite qu'elles soient supprimées car **[motif_de_la_suppression].**
Je vous remercie également de faire le nécessaire pour que ces pages ne soient plus référencées par les moteurs de recherche (art. 17.2 du RGPD). Vous voudrez bien me faire parvenir votre réponse dans les meilleurs délais et, au plus tard, dans un délai d'un mois à compter de la réception de ma demande (art. 12.3 du RGPD).
Je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées.

Fait à…, le…
Signature

Fiches pratiques

SUPPRIMER DU CONTENU SUR 6 RÉSEAUX

À chaque site, sa méthode d'effacement… Les démarches pour chacun d'entre eux.



GOOGLE

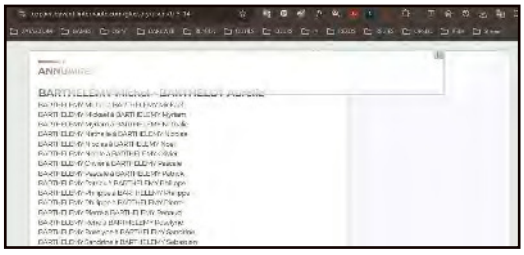
1 **Connectez-vous** à la page « Trouble shooter »[1]
2 **Sélectionnez** le lien Google diffusant l'information à faire disparaître
3 **Indiquez** l'URL incriminée et votre identité (pour éviter les fausses demandes)

YAHOO !

1 **Connectez-vous** à la page « Contact »[4]
2 **Sélectionnez** « Envoyer un mail à un spécialiste »
3 **Précisez** votre pays, votre adresse électronique, l'adresse incriminée et/ou le terme à faire disparaître

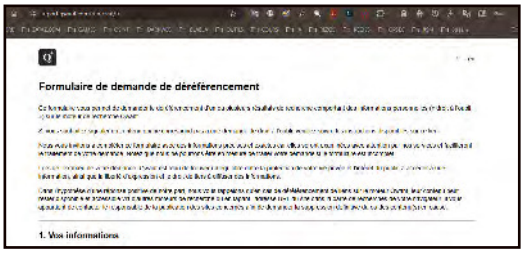
BING (MICROSOFT)

1 **Connectez-vous** à la page « Privacy Request »[2]
2 **Choisissez** « Je suis la personne dont le nom apparaît dans les résultats de recherche »
3 **Fournissez** l'URL et votre identité



COPAINS D'AVANT

1 **Connectez-vous** à votre compte et cliquez sur « Gérer mes préférences »
2 **Allez** dans la rubrique « Sécurisation de mon profil »
3 **Décochez** « Permettre à mes Copains d'avant de me trouver via les moteurs de recherche »



QWANT

1 **Connectez-vous** à la page « Removal »[3]
2 **Sélectionnez** le motif de la demande
3 **Indiquez** l'URL et votre identité

TIKTOK

1 **Allez** sur le profil de la vidéo à faire retirer
2 **Cliquez** sur l'icône « Signaler »
3 **Allez** sur « Publication de contenu inapproprié » et choisissez la raison du signalement

(1) Support.google.com/legal/troubleshooter/1114905.
(2) Bing.com/webmaster/tools/eu-privacy-request.
(3) Report.qwant.com/removal/fr. **(4)** *Io.help.yahoo.com/contact.*

Le smartphone
VOTRE MEILLEUR ENNEMI

Savez-vous ce que votre téléphone sait de vous ? Il peut expédier sur des serveurs distants, en une demi-journée seulement, tout un tas d'informations… et de détails intimes sur votre vie.

En 2021, le chercheur en sécurité informatique Doug Leith (université de Dublin, Irlande) révélait une collecte inquiétante: toutes les 4 minutes 30, votre smartphone transfère à des entreprises (constructeurs, opérateurs, éditeurs d'applications…) des dizaines de vos données personnelles (géolocalisation, numéro de téléphone, identifiant de carte SIM, etc.), souvent à votre insu. Quatre ans plus tard, le phénomène s'est accentué. Pour vous donner une idée de son ampleur, j'ai élaboré ci-dessous une journée type avec mon «meilleur ennemi»… qui pourrait ressembler à la vôtre à bien des égards.

▶ *Le matin*

Au réveil, j'allume mon smartphone. Après la connexion automatique avec mon opérateur, une synchronisation s'opère avec ma montre connectée. Elle lui livre un rapport sur mon sommeil: des données sur sa durée, ses phases, mon rythme cardiaque… tout y passe. En arrière-plan, mes applis se mettent à jour. Les actualités du matin défilent, calibrées par l'algorithme selon mes habitudes de lecture. Comme il connaît ma date de naissance, il me fournit aussi mon horoscope, avant de «pousser» une pub (notification push) pour une consultation de voyance payante. Grâce à la géolocalisation active, la météo locale s'affiche, ainsi que le trafic routier dans ma zone. Mon appli de courses m'informe qu'il n'y aura plus de lait demain si je ne clique pas sur «Acheter». Je file ensuite sur Instagram, et mes contacts voient que je suis en ligne. Tandis que je scrolle un peu sur mon fil, des robots analysent mes likes afin de m'inonder de contenus similaires. Message de mon opérateur de téléphonie mobile: ma ligne, tombée en panne cette nuit, est revenue à la normale. Son intelligence artificielle (IA) me souhaite une «*Belle journée*».

Votre téléphone connaît tous vos déplacements et vos habitudes d'usage. Mais attention, c'est un mouchard !

PETERHOWELL/ISTOCK

En chemin vers le bureau

Je monte dans ma voiture, direction le bureau. Mon GPS, qui me guide, me prévient d'un accident à cinq minutes de chez moi. L'application Waze me propose alors le meilleur itinéraire pour atteindre mon travail à partir des 4000 téléphones connectés autour de moi. Je dois prendre le métro? J'active le système de paiement sans contact (NFC) et règle mon ticket dématérialisé. Dans le tunnel, je me connecte au wifi gratuit: la RATP récupère alors mon numéro de téléphone, le nom de mon appareil et ma position. Un peu plus loin, contrôle des billets: l'agent approche son terminal de mon smartphone, vérifie la validité de mon titre et me remercie d'un chaleureux *«Bonne journée monsieur Bancal!»*. Il connaît mon identité grâce à son boîtier… Hier, dans la rame, un ami a repéré ma présence quand «Wifi Téléphone Damien» est apparu sur son écran.

À la pause déjeuner

Alors que je passe devant une boutique, mon smartphone se met à vibrer. Une application m'envoie en temps réel une promo pour 15 litres de soda. Dans mes écouteurs Bluetooth, mon appli musicale sélectionne non seulement mes titres favoris, mais analyse également l'environnement sonore, afin de me proposer des morceaux «dans l'air du temps». Mon téléphone se repère dans l'espace et m'indique la météo de l'endroit précis où j'arrive. Mon historique Google (à l'instar de celui d'Apple) me rappelle que je suis un fidèle de ce lieu et me propose de lui donner un avis étoilé. Un sondage Google m'offre de l'argent si je réponds à des questions liées à ma consommation actuelle.

Au cours de l'après-midi

Vers 15 heures, je me connecte à ma banque, qui me réclame une authentification à deux facteurs pour autoriser l'accès à mon compte. Mon numéro de téléphone et parfois même mon code Imei (identifiant unique du mobile) lui sont envoyés. Peu après, je contacte mon conseiller bancaire. Je n'ai pas besoin de me présenter quand il décroche. Un peu comme avec le pirate qui a tenté de m'arnaquer hier soir. Lui aussi savait à qui il s'adressait, grâce aux données d'entreprises collectées ces dernières semaines sur le dark web.

Dans la soirée

Retour à la maison. Ma box TV connectée me suggère une sélection de *«films qui devraient [me] plaire»*. Trois sur cinq sont payants; l'achat de celui que je choisis est validé d'un clic. Il n'est pas nécessaire que je saisisse ma carte bancaire, elle est déjà stockée. L'IA de Netflix ou d'Amazon Prime va jusqu'à générer des «affiches» de séries et de films qui sont censés m'intéresser. Je jette un œil aux aliments stockés dans mon frigo et demande à ChatGPT de me donner une recette rapide, que j'envoie à mon robot de cuisine connecté tout en réunissant les ingrédients. Avant de dormir, je me lave les dents avec une brosse à dents connectée – cette rapporteuse transmet à mon smartphone les zones mal nettoyées! Celui-ci me signale qu'une mise à jour de sécurité est disponible; il est recommandé de l'installer pendant la nuit pour éviter des failles exploitables par des pirates. Avant l'extinction des feux, je reçois un dernier SMS: une pub du constructeur de mon mobile qui m'en offre un neuf à moitié prix… à condition de renvoyer l'ancien, avec toutes mes données dessus… que je ne sais pas effacer à 100%.

COMMENT LIMITER LA FUITE ?

Il faut restreindre les autorisations. Pour cela, allez dans les paramètres, désactivez l'accès aux données non essentielles (géolocalisation, microphone, contacts…). N'oubliez jamais de fermer les connexions inutiles comme le NFC, le Bluetooth, le wifi et le GPS. Mettez à jour votre appareil et vos applications sans tarder, cela corrige les failles avant qu'elles ne soient exploitées. Effacez toutes les applications que vous n'utilisez pas ou très peu. Vous souhaitez revendre votre appareil ou profiter des «promotions» reprise? Ma politique est la destruction et le recyclage des pièces. Chiffrez vos fichiers puis détruisez-les, et réinitialisez votre engin en mode usine. ■

MORALITÉ

En une journée, votre smartphone en sait plus sur vous qu'un ami d'enfance. Et il parle… beaucoup.

Enfants
LA SÉCURITÉ EN JEU

Jeux vidéo, réseaux sociaux, applis éducatives… les mineurs laissent chaque jour une empreinte numérique massive, qui attire autant les marques que les escrocs. Si un cadre légal existe, il se confronte à une certaine réalité.

Le Règlement général sur la protection des données (RGPD) a posé un cadre, mais son application aux enfants reste un défi. D'autant que la consommation des mineurs change aux grés des modes, plusieurs fois par an, si ce n'est plusieurs fois par mois. Les vidéos ultracourtes (TikTok, Réels, Shorts) et les carrousels dynamiques [qui permettent d'afficher plusieurs contenus dans un seul post] captent plus que jamais l'attention de ce public pressé. Les plus jeunes ont du mal à s'extraire des buzz toxiques… sans parler des trucages issus de l'intelligence artificielle (IA) générative. En 2025, toutefois, des plateformes axées sur la bienveillance, la décentralisation (Mastodon, Bluesky…) et la collaboration ont émergé.

UN CADRE LÉGAL CLAIR

Dans l'Union européenne, il faut avoir 16 ans pour pouvoir consentir seul au traitement de ses données personnelles, sauf dans certains pays, où ce seuil a été abaissé: 15 ans en France, 13 ans en Irlande, Espagne, Pologne… Quoi qu'il en soit, les parents ou les tuteurs légaux doivent aussi donner leur accord. Le RGPD impose également de limiter la collecte à celles qui sont strictement nécessaires; de sécuriser les informations stockées; d'informer clairement les parents et les enfants de leurs droits; de faciliter l'accès, la rectification et la suppression des données.

LES RÉSEAUX SOCIAUX CONCERNÉS

Ces règles s'appliquent à toutes les structures traitant des données d'enfants européens, où qu'elles siègent dans le monde. Les réseaux sociaux en font partie. Ils sont donc tenus de fixer un âge minimum à leurs utilisateurs, de proposer des politiques de confidentialité adaptées et de lutter contre le harcèlement, la désinformation et les contenus inappropriés. Mais ce n'est pas toujours le cas… L'éditeur de jeux vidéo Epic Games a ainsi écopé, en 2022, de plus de 443 millions d'euros d'amende par la Federal Trade Commission (FTC) américaine pour violation de la loi sur la protection de la vie privée des enfants en ligne (Coppa). Motif: dans les jeux *Fortnite* et *Rocket League,* des mineurs avaient la possibilité de participer à des tchats vocaux sans validation parentale.

En juillet 2023, la France a voté une loi instaurant une «majorité numérique» à 15 ans: en dessous, les jeunes ne peuvent accéder aux réseaux sociaux qu'avec l'accord de leurs parents et via des mécanismes de vérification d'âge. Sauf que faute de décret d'application et du feu vert de la Commission européenne, cette mesure est restée en suspens… L'exécutif serait susceptible de passer outre en 2026 si Bruxelles ne bouge pas, et d'intégrer les actions menées par l'Australie depuis 2024. Ce pays a en effet adopté, l'année dernière, l'Online Safety Amendment (Social Media Minimum Age) Bill, qui interdit aux moins de 16 ans de créer des comptes sur la plupart des réseaux sociaux, dont Facebook, Instagram, TikTok, Snapchat, Reddit, YouTube et X. Ce texte a pris effet en décembre 2025. Seules sont exemptées les applis à vocation éducative ou sanitaire, comme YouTube Kids, Google Classroom, WhatsApp, Messenger Kids ou encore la plateforme d'aide pour la jeunesse Headspace. Pour définir les *reasonable steps* («attendus raisonnables») des

Si le mineur n'a pas 16 ans, ses données personnelles ne peuvent pas être collectées sans l'accord des parents… en théorie.

plateformes, la eSafety Commissioner australienne mène des consultations sur leurs technologies d'identification d'âge (estimation faciale, données mobiles ou bancaires, etc.). Un travail également réalisé dans l'Hexagone, où plusieurs sites pour adultes ne se conformant pas au contrôle rigoureux de l'âge ont été bloqués en 2025.

DES SAFE ZONES POUR JOUER SANS DANGER ?

La prévention passe, en outre, par des initiatives. En novembre 2022, l'opérateur Orange a déployé des *safe zones* («zones sécurisées») dans les jeux *Fortnite, Roblox* et *Minecraft,* très prisés des ados, afin de leur permettre de poser des questions en toute sécurité. Or, en 2025, sur les 400 mineurs croisés par votre journaliste dans les ateliers de sensibilisation qu'il mène dans les écoles, un seul avait visité cet espace virtuel sur *Fortnite*… Il suffit pourtant au joueur de placer son avatar sur le bouton *Jump to talk* («sauter dessus pour parler») pour alerter un robot, recevoir des conseils et, si besoin, être orienté vers le 3018, le numéro national gratuit, anonyme et confidentiel dédié aux victimes de cyberharcèlement et autres violences numériques. ■

ATTENTION À LIKEE !

On en parle peu, mais cette plateforme d'origine singapourienne est à garder à l'œil. Likee est un réseau social lancé en juillet 2017 par l'entreprise Bigo Technology (elle-même filiale du groupe chinois Joyy Inc.). Ce «petit TikTok» est orienté vidéos courtes. Comme chez son grand frère, la monétisation y est omniprésente, incitant nombre de contributeurs à dépasser des limites (respectées par les concurrents) en matière de violence, de grossièreté ou encore de nudité. La plateforme a mis en place des contrôles parentaux et des avertissements sur certains contenus, mais elle est régulièrement critiquée pour l'accès trop facile des mineurs à des vidéos inappropriées. En outre, le profilage publicitaire y est pratiqué : on y saisit vos données biométriques, votre localisation, vos habitudes d'usage…

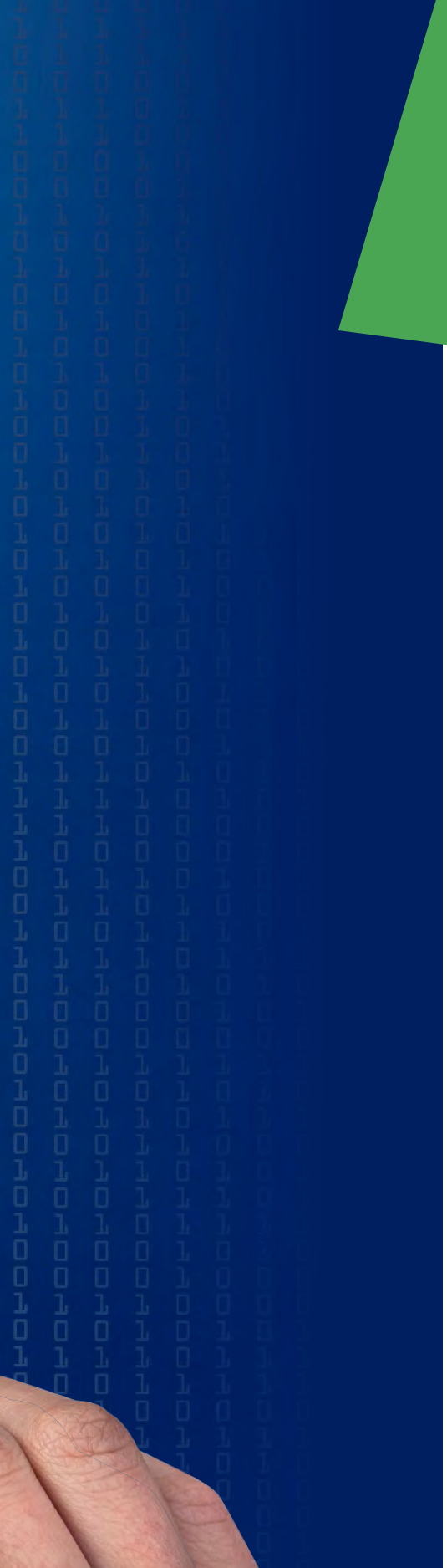
D. STANKOVIC/ISTOCK


71%

L'identité numérique

Protéger ses mots de passe, maîtriser son identité en ligne, sécuriser le partage d'informations sensibles: adopter chaque jour les bons gestes numériques s'avère vital. Car les pirates n'attendent qu'une occasion pour frapper. Les cyberattaques mondiales ont bondi de 15% en un an. En France, la Cnil a été notifiée de 5629 violations de données personnelles en 2024, soit 20% de plus qu'en 2023. Fin mai 2025, Cloudflare a repoussé une attaque DDoS (faux trafic internet pour submerger un site) culminant à 7,3 Tbps, un record. Ces chiffres traduisent l'intensité des cybermenaces. Dans ce chapitre, vous apprendrez à fabriquer votre couteau suisse de cybersécurité, un kit d'astuces et de réflexes simples pour garder une longueur d'avance.

SOMMAIRE



EXENTIA ; N. EINO/ADOBE STOCK

5 règles d'or POUR SURFER SANS RISQUE

Les cyberattaques sont de plus en plus sophistiquées, ciblées et dures à déceler ! Voici cinq pratiques essentielles et éprouvées pour protéger son identité numérique, accompagnées d'exemples concrets.

1 CHOISIR DES MOTS DE PASSE SOLIDES… ET UNIQUES

Un mot de passe faible, c'est l'équivalent numérique d'une serrure rouillée: elle donne l'illusion de protéger, mais cède au premier coup de tournevis. Un logiciel de *brute force* utilisé par un cybercriminel est capable de tester des millions de combinaisons par seconde. Des codes trop simples comme «123soleil» ou «azerty» sautent alors immédiatement. La bonne pratique consiste à choisir, pour chacun de ses comptes, un mot de passe unique, suffisamment long (15 caractères minimum) et construit avec un mélange de lettres majuscules et minuscules, de chiffres et de symboles, par exemple «F ! lm0n_S3cur1t3_2025». Se servir d'un code difficile à casser est indispensable, car l'inverse peut coûter très cher ! En 2024, un forum de passionnés d'automobiles a subi une fuite de données. Les identifiants compromis ont permis aux pirates de se connecter aux boîtes mails de ses membres, dont certains utilisaient les mêmes codes ailleurs, y compris sur leur espace bancaire… qui s'est retrouvé vidé. Pour éviter ce scénario, servez-vous d'un gestionnaire de mots de passe, qui en génère et en stocke de forts et uniques: les sites de Bitwarden, la Cnil [1], 1Password [2] ou KeePassXC sont ici recommandés.

2 OPTER POUR UNE PASSKEY, LA MEILLEURE SOLUTION ?

Depuis 2023, Apple, Google et Microsoft poussent à l'adoption de *passkeys,* ou «clés de connexion». Cette technologie d'authentification ne nécessite plus de mot de passe. Votre appareil (smartphone, tablette, ordinateur) stocke une clé cryptographique unique, liée à votre compte, et vous vous authentifiez par reconnaissance biométrique (empreintes, visage) ou code PIN local. Cela supprime deux risques majeurs, les fuites de bases de données contenant des mots de passe (attention, cela ne stoppe pas une fuite en cours, nous y reviendrons) et les attaques par hameçonnage (phishing) qui visent à vous soutirer vos identifiants. Imaginons ainsi qu'un faux site bancaire tente de vous piéger via un formulaire imitant l'original: avec une *passkey,* même si vous avez cliqué sur un lien frauduleux, l'escroc reste techniquement incapable de valider l'authentification, car il ne détient pas la clé privée stockée sur votre

RESTEZ VIGILANT !

L'hameçonnage (phishing) n'arrive pas qu'aux autres. En 2024, la majorité des cyberattaques réussies en France ont commencé par un courriel frauduleux. Les pièges sont de plus en plus crédibles: un logo parfait, un ton «administratif» rassurant, une adresse électronique presque correcte… et l'IA qui, maintenant, aide les pirates. Certains signes doivent vous inciter à jeter l'e-mail : le nom de domaine est suspect ou déformé ; les liens pointent vers une autre adresse que celle affichée ; on vous demande de vite vérifier ou confirmer un compte ; l'adresse physique ou les mentions légales manquent. Règle d'or, ne cliquez pas et ne téléchargez aucun fichier depuis un message inattendu. En cas de doute, contactez l'entreprise ou l'administration par un canal officiel et, surtout, ne donnez jamais vos identifiants à un tiers.

Activez la double authentification pour renforcer votre sécurité !

FERRANTRAITE/ISTOCK

appareil… Attention, cette solution n'est pas imparable ! Aujourd'hui, les pirates n'hésitent plus à vous téléphoner – voire, dernière tendance, à vous faire appeler un numéro que vous pensez légitime. De plus en plus de plateformes (eBay, PayPal, GitHub) permettent d'activer cette option; en 2025, c'est une arme très efficace, surtout sur vos comptes sensibles.

3 L'AUTHENTIFICATION, VOTRE GARANTIE ANTI-INTRUSION

Même avec un mot de passe en béton ou une *passkey,* il est prudent d'ajouter une vérification supplémentaire, en utilisant un système *multi-factor authentication* (MFA) ou *two-factor authentication* (2FA). Le principe: combiner, pour vous connecter à un compte, quelque chose que vous savez (mot de passe) et quelque chose que vous possédez (un code cryptographique temporaire généré par une application, une clé physique, etc.). Un peu fastidieux, mais très utile ! En 2025, un pirate a réussi à obtenir le mot de passe d'un haut responsable de la compagnie aérienne russe Aeroflot; tous les avions du transporteur sont donc restés au sol… Si ce directeur s'était servi d'un système 2FA, la connexion illégitime aurait été bloquée. Bref, pour une sécurité maximale, recourez à une application d'authentification – Authy, Google Authenticator ou Microsoft Authenticator [3] – ou à une clé de sécurité matérielle FIDO2/WebAuthn [4] (YubiKey, SoloKeys). Évitez les codes envoyés par SMS ou courriel, beaucoup plus faciles à intercepter.

4 MISES À JOUR ET SAUVEGARDES : DES CYBERASSURANCES-VIE

Chaque mois, des centaines de failles de sécurité sont découvertes dans les systèmes d'exploitation Windows, MacOS, Android ou iOS et dans les applications. Les mises à jour permettent de corriger ces vulnérabilités, notamment celles exploitables immédiatement après leur divulgation – telle celle apparue sur le logiciel de messagerie WhatsApp, en 2025, qui donnait à un pirate la possibilité d'exécuter un code malveillant rien qu'en envoyant un message piégé, sans même que les utilisateurs ne cliquent sur le fichier joint ou le lien… Une simple mise à jour a rendu cette >>

>> faille inopérante, en plus d'ajouter de nouvelles fonctionnalités à l'appli. N'oubliez pas, en parallèle, de sauvegarder vos données sur un support externe ou un espace virtuel (cloud) sécurisé. En cas d'attaque par ransomware (logiciel malveillant qui piège vos données contre une rançon), vous pourrez restaurer vos fichiers sans payer.

5 LE VPN, UN BOUCLIER NOMADE

Un *virtual private network* (VPN, ou «réseau privé virtuel») chiffre votre connexion et masque votre adresse IP (numéro d'identification unique attribué à chaque appareil connecté à Internet, lire aussi p. 42). Cela complique le suivi de vos activités par un escroc et empêche ses interceptions de messages, comme ça arrive parfois sur les réseaux publics – wifis gratuits d'aéroport, de restaurant, d'hôtel, de camping, de maison d'hôtes… –, où vos données ne sont pas chiffrées. Avec un VPN, les flux sont illisibles et inutilisables. Mais attention ! Ce n'est pas une cape d'invisibilité. Le fournisseur de VPN, lui, connaît votre identité et vos codes de connexion. Donc, choisissez-en un réputé, avec une politique stricte de non-conservation des historiques, aussi appelés logs – Proton VPN [5], VyprVPN [6] –. Et méfiez-vous de ceux qui communiquent beaucoup en proposant des mois de gratuité pour vous attirer: il n'y a pas de cadeau dans la vie numérique ! ■

(1) Cnil.fr/fr/generer-un-mot-de-passe-solide. (2) 1password.com/fr/password-generator. (3) Microsoft.com/fr-fr/security/mobile-authenticator-app. (4) Normes technologiques de clé de sécurité. (5) Protonvpn.com. (6) Vyprvpn.com.

Un réseau privé virtuel (VPN) chiffre votre connexion.

PRYKHODOV/ISTOCK

QUATRE RAPPELS DE SÉCURITÉ

> **Segmentez vos adresses électroniques** Créez une messagerie distincte par usage – par exemple, une pour l'administration, une pour vos achats en ligne, une pour vos loisirs. Cela limite l'impact en cas de fuite de données, une compromission n'exposera pas tous vos comptes. Des solutions comme Proton Mail proposent de créer des adresses anonymisées.

> **Adoptez des mots de passe en béton** Ils doivent comporter au minimum 15 caractères avec majuscules, minuscules, chiffres et symboles. Évitez les références personnelles (date de naissance, prénom d'un proche) et utilisez un gestionnaire de mots de passe pour les retenir à votre place.

> **Activez la double authentification** Avec cette vérification supplémentaire (code fourni par une appli, clé USB de sécurité…), même si votre mot de passe est volé, la situation ne sera pas catastrophique. Le principe est connu depuis longtemps. Dans le film *Le cercle rouge*, réalisé par Jean-Pierre Melville en 1970, Alain Delon, Gian Maria Volonté et Yves Montand cherchent à neutraliser le dispositif de sécurité d'une bijouterie, place Vendôme, où deux serrures distinctes doivent être ouvertes et synchronisées avec la désactivation d'une alarme… En 1996, on retrouve une «2FA» dans *Mission : Impossible* de Brian De Palma : la salle blanche de la CIA n'est accessible qu'en plusieurs étapes, dont un accès par double autorisation. Tom Cruise le sait et préfère passer par le plafond !

> **Naviguez sous protection** En déplacement, connectez-vous via un VPN fiable. Il chiffre vos données et rend vos connexions illisibles pour les curieux. Attention : vous ne devenez pas anonyme avec un VPN, mais il complique grandement le suivi de votre activité.

VISEZ LA CYBERPROTECTION

Collecter les données personnelles des autres, c'est une responsabilité. Nos conseils pour le faire sans perdre la confiance de ceux qui vous les confient.

Le Règlement général sur la protection des données (RGPD) ne concerne pas que les géants du Web. Vous êtes une petite association de quartier ou un artisan indépendant ? Vous y êtes aussi soumis. Règle d'or: ne demander à vos clients/adhérents que ce qui est strictement nécessaire à votre fonctionnement. Par exemple, si vous avez monté un club de randonnée, vous n'avez pas besoin de connaître la profession ou le médecin traitant de vos membres, sauf exigence médicale précise.

La Commission nationale de l'informatique et des libertés (Cnil) insiste: définissez un but clair, légitime, explicable… et ne déviez jamais de cet objectif. Nom, prénom, adresse, numéro de téléphone, e-mail… ces éléments paraissent banals, mais entre de mauvaises mains, ils risquent d'être exploités à des fins d'usurpation d'identité ou de harcèlement. Vous êtes tenu d'informer les personnes concernées, de les prévenir de l'usage prévu pour leurs données et de leur expliquer comment elles peuvent exercer leurs droits. Ne collectez jamais un renseignement à leur insu: c'est illégal. Et, s'il s'agit de mineurs, demandez l'accord d'un représentant légal, c'est obligatoire. Par ailleurs, les données personnelles ne doivent pas être gardées éternellement. Fixez une durée maximale, communiquez-la et respectez-la. Par exemple, des fiches d'inscription seront stockées un an puis détruites, anonymisées ou archivées, conformément aux règles en vigueur. Conserver « au cas où » est interdit et passible de sanctions. Selon son rapport d'activité annuel publié en avril 2025, la Cnil a reçu 17 772 plaintes pour violation de données personnelles en 2024.

Assurez vos arrières

Sécurisez vos équipements, qu'il s'agisse de locaux, d'armoires ou d'ordinateurs. Limitez l'accès aux seuls employés autorisés. Chiffrez les données sensibles et sauvegardez régulièrement: après un piratage ou un incendie, c'est souvent la seule façon de repartir. Enfin, rappelez-vous qu'un cloud sans mot de passe solide ou un disque dur laissé sans protection sont des portes ouvertes aux fuites (lire également p. 38). ■

EFFACER DÉFINITIVEMENT VOS TRACES DANS META

Avant toute suppression, regardons comment sauvegarder vos données :

> **Sur Facebook** Allez dans « Paramètres ». Cherchez « Vos informations Facebook » puis « Télécharger vos informations » ;

> **Sur Instagram** « Paramètres > Votre activité > Télécharger vos informations » ;

> **Sur Messenger** Rien à faire, les conversations sont incluses dans la sauvegarde Facebook.

> **Supprimer son compte Facebook** Dans « Paramètres », allez dans « Vos informations Facebook » puis « Désactivation et suppression ». Sélectionnez « Supprimer définitivement » et « Confirme avec ton mot de passe ». Un lien direct existe aussi : Facebook.com/help/delete_account. Vous avez ensuite 30 jours pour revenir en arrière et annuler la suppression. Sinon, l'effacement se fait en 90 jours max.

> **Supprimer son compte Instagram** Allez sur Instagram.com/accounts/remove/request/permanent/ depuis un navigateur. Connectez-vous sur « Sélectionne la raison > Saisis ton mot de passe > Valider ». Le délai d'annulation est de 30 jours.

> **Supprimer Messenger** La suppression de Facebook entraîne automatiquement celle de Messenger.

Vos données LE NOUVEL OR NOIR DES PIRATES

Adresses électroniques, mots de passe, numéros de téléphone… se volent, se monnayent et s'utilisent à des fins frauduleuses. En 2024 et 2025, les cybercriminels n'ont jamais été aussi actifs.

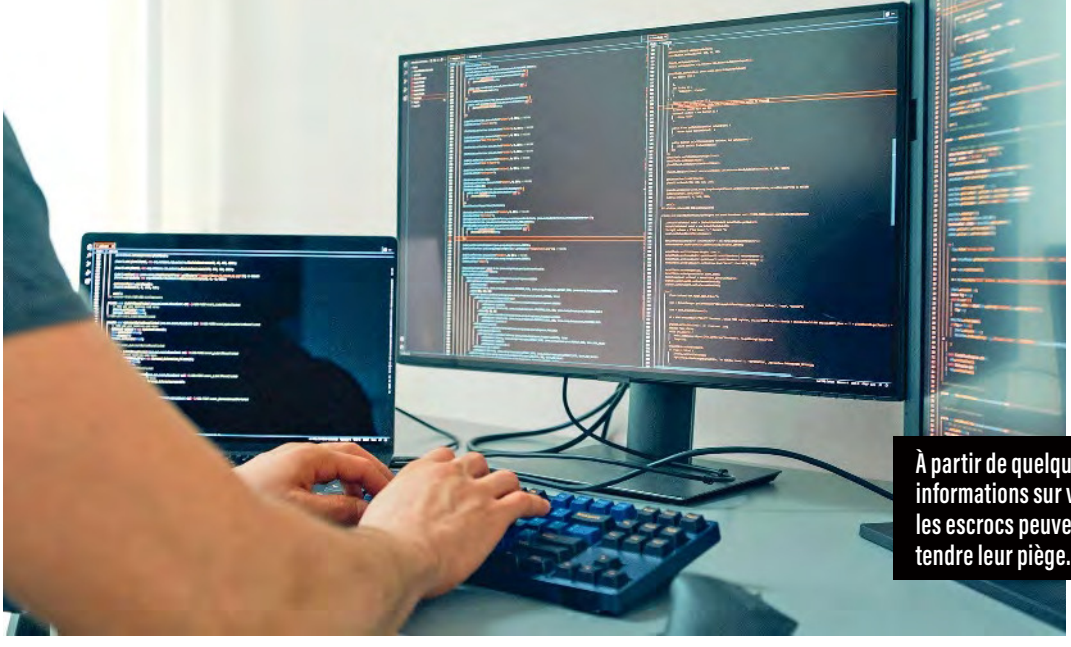
Les gendarmes du Net observent chaque semaine des fuites massives de données: messageries, mots de passe, numéros de téléphone, parfois accompagnés de détails plus sensibles comme l'adresse postale ou la date de naissance. Et ces informations, loin de dormir dans un coin du Web, se revendent, se croisent, s'exploitent. Un pirate peut, à partir de quelques données banales, remonter jusqu'à vos comptes en ligne, usurper votre identité ou préparer une arnaque sur mesure. Des chiffres qui donnent le vertige: 91% des professionnels de la cybersécurité estiment que les attaques dopées à l'IA vont exploser d'ici à 2028… mais seuls 26% se disent prêts à les détecter (source: Zataz). Une donnée volée peut être utilisée près de 100 fois en moins de 5 minutes! En France, la plateforme gouvernementale Cybermalveillance.gouv.fr a constaté une hausse de 49,9% des demandes d'assistance en 2024 par rapport à 2023, avec en tête la violation de données personnelles (+ 82% des demandes), le piratage de comptes (+ 47%) et les escroqueries en ligne.

Pourquoi vous êtes une cible

En France, et cela depuis 1978, la Commission nationale de l'informatique et des libertés (Cnil) définit une donnée personnelle comme toute information se rapportant à une personne physique identifiée ou identifiable. Individuellement, ces données semblent anodines. Mais, croisées, elles constituent un passeport pour le cybercrime. L'internaute doit donc en conserver la maîtrise. Si ce n'est pas le cas et qu'il se les fait dérober, il peut se retrouver identifié directement (via son nom et son prénom), indirectement (par son numéro de téléphone ou de Sécurité sociale, sa plaque d'immatriculation, son adresse postale ou e-mail, mais également sa voix et son image), ou encore par croisement (par exemple: date de naissance + adresse postale + nom de famille). Son identité établie fait de lui une potentielle cible de cyberattaque.

Les bonnes pratiques, ça doit devenir automatique

Les pirates ne dorment jamais et leurs pièges sont souvent simples, donc redoutables. La meilleure protection? Des gestes clairs, faciles à adopter, appliqués systématiquement. Hélas, trop de gens les oublient. Alors, répétons-les: un mot de passe fort et unique pour chaque compte en ligne; la double authentification (2FA) activée sur les services sensibles; pas de clic sur un lien reçu dans un message suspect (75% des vols d'informations commencent ainsi); des mises à jour régulières des logiciels et des appareils pour colmater les failles; un antivirus actif sur tous les équipements, y compris le smartphone; aucune donnée personnelle partagée sur des réseaux sociaux publics ou des sites non sécurisés; le VPN obligatoire sur wifi public (café, hôtel, salle de sport); pas d'utilisation d'ordinateurs publics ou partagés, même brièvement; la création d'une liste des sites et d'organismes qui détiennent vos données afin de garder la main dessus. Enfin, dans tous les cas, vous ne sauriez trop réfléchir avant de divulguer une information personnelle. Par exemple, avez-vous absolument besoin de donner votre adresse postale à ce site, alors que vous n'y commandez rien? Ou encore, faut-il vraiment communiquer, comme on vous le demande sur ce formulaire pour télécharger un livre blanc qui vous intéresse,



MSTOCK/ISTOCK

À partir de quelques informations sur vous, les escrocs peuvent tendre leur piège.

vos nom, prénom, adresse électronique et numéro de téléphone ? Imaginez toujours que ces renseignements, notamment votre 06, pourront être ajoutés à des bases de démarchage, voire destinés à des tentatives de phishing vocal (vishing). Le bon réflexe, ici, serait de ne fournir qu'une adresse mail, idéalement dédiée à ce type d'inscription.

En prenant ces précautions, vous maximiserez la protection de votre vie privée et de votre sécurité en ligne. Rappelons également que toute personne a le droit de réclamer les informations qu'elle a livrées au délégué à la protection des données (DPO) d'un site, afin de les réutiliser ou de les transmettre à un autre responsable (art. 20 du Règlement général sur la protection des données). Le DPO, lui, est censé répondre sous un mois, même lorsque son entreprise ou organisme ne dispose d'aucune data sur le demandeur. ■

GÉREZ VOS INSCRIPTIONS

Créez un tableau sur papier, tableur Excel, etc. (exemple ci-dessous) afin de regrouper toutes les informations que vous divulguez lors de vos inscriptions sur des sites. En cas de besoin, vous saurez qui a quoi. Et, surtout, qui contacter pour faire valoir vos droits. Nous vous conseillons en effet d'inclure à cette base les adresses mails des responsables du traitement des données (DPO) des portails web que vous fréquentez. Ce tableau devra être mis à jour après chaque nouvelle inscription ou modification de données. Vérifiez régulièrement que la messagerie du DPO est toujours valide et visible dans la politique de confidentialité du site. Enfin, archivez les comptes fermés avec la date de suppression et la confirmation reçue.

SITES INTERNET QUI SAIT QUOI SUR VOUS ?

EXEMPLES	INSCRIPTION	DONNÉES FOURNIES	COMPTE	CONTACT RGPD/DPO	CONTRÔLE
AMAZON	15/01/2025	Nom, prénom, adresses mail et postale	Achat en ligne	dpo@amazon.fr	05/08/2025
RÉSEAU SOCIAL X	03/07/2024	Nom, photo, date de naissance, e-mail	Réseau social	dpo@reseauxocial.com	12/05/2025
BANQUE Y	21/11/2023	Nom, prénom, téléphone, e-mail, RIB	Banque en ligne	dpo@banquey.fr	01/04/2025

Vos photos EMPLOI ILLICITE DE VOTRE PORTRAIT

Les fuites de données personnelles ne concernent pas que les numéros de téléphone ou les adresses mails. La preuve… par l'image.

Votre identité numérique, c'est aussi votre photo – et elle peut être utilisée à votre insu. Imaginez: un cliché de vous, pris lors d'une soirée en boîte de nuit, se retrouve sur le site et les réseaux sociaux de l'établissement. Accepteriez-vous de servir de panneau publicitaire gratuit ? Voici quelques outils pour repérer les usages non expressément autorisés de votre image, identifier les responsables et reprendre le contrôle.

PimEyes

Développé par une société polonaise, PimEyes est un moteur de recherche spécialisé, capable de détecter les espaces en ligne qui exploitent indûment votre portrait. À partir d'une simple photo, il repère en quelques secondes les sites où elle apparaît, y compris si elle a été modifiée (passée en noir et blanc, colorisée, recadrée…). L'outil, accessible sur Pimeyes.com, fonctionne gratuitement pour la recherche sur le Web ouvert. Sa base indexe plus d'un milliard de clichés sous forme de signatures biométriques (pas d'images directes). Efficace… et controversé. Aucune inscription n'est nécessaire pour l'utiliser, ce qui permet à n'importe qui de lancer une recherche à partir d'une photo qui ne lui appartient pas. Une option payante étend la recherche au deep Web (des sites accessibles mais non référencés). Son concurrent américain, Clearview AI, réservé aux autorités, revendique plus de 3 milliards de visages analysés !

Google Images

Le moteur de recherche de Google dispose d'une fonction dédiée à l'analyse des photos (Images.google.com). Le principe: cliquer sur l'icône appareil photo, importer l'image à analyser, puis obtenir en quelques secondes la liste des sites qui s'en servent. De nouvelles règles, plus drastiques, permettent d'éviter l'usage abusif d'un portrait. Les recherches sont limitées. Il est possible de recadrer le cliché afin de supprimer des éléments perturbateurs (bâtiments, objets, personnes…), ce qui améliore la détection par l'algorithme.

Vos photos peuvent être exploitées à votre insu. Prudence si vous les publiez sur les réseaux sociaux.

L'IA ET VOTRE PHOTO
UN RISQUE EXPONENTIEL

Avec l'essor fulgurant de l'intelligence artificielle (IA) générative, une simple photo de vous peut servir à créer un deepfake (vidéo ou photo réaliste mais falsifiée) à caractère diffamatoire ou compromettant. Et aussi à générer des clones numériques à votre image, qui seront mis en scène dans des campagnes frauduleuses (arnaques vidéo, usurpation sur visioconférence…). Pour vous prémunir contre de telles situations, limitez la diffusion publique de vos clichés, privilégiez les réseaux où vous contrôlez les paramètres de confidentialité et surveillez régulièrement l'usage de votre portrait via des systèmes de recherche inversée. Enfin, ne mettez pas votre visage dans un outil IA !

L'intelligence artificielle permet de créer des contenus falsifiés (deepfakes) avec un simple cliché.

Forensically

Conçu en 2015 par un ingénieur suisse nommé Jonas Wagner, Forensically (29a.ch/photo-forensics) est un outil gratuit, en anglais, dédié à l'analyse médicolégale d'images. Il ne localisera pas votre portrait sur Internet, mais décèlera les modifications qu'il a subies: retouches, clonages, ajouts d'objets ou de décors… En bref, n'importe quel signe de manipulation. Un moyen supplémentaire de garder la main sur votre image et de vérifier l'authenticité des clichés qui circulent.

Lenso.ai

Cette plateforme polonaise a été créée en 2024. Elle est spécialisée dans la recherche inversée d'images, y compris la reconnaissance faciale. Elle se distingue par sa fonction d'alerte, qui notifie l'utilisateur lorsqu'un visage similaire est repéré en ligne.

FaceCheck.ID

Ce moteur de recherche facial se révèle efficace, notamment pour trouver des personnes sur les réseaux sociaux. Il constitue un très bon complément à PimEyes.

TinEye

En lançant une recherche sur cette plateforme, vous accédez à plus de 78,7 milliards d'images et avez la possibilité de les localiser en ligne. Son utilisation est privée, et TinEye n'enregistre pas vos images de recherche.

ProFaceFinder

Bien que non spécialisé en reconnaissance faciale, cet outil de recherche inversée d'images s'avère rapide et fiable. Il excelle à repérer le site où une photo apparaît, même si des modifications y ont été opérées.

Face Search AI

Ce service de reconnaissance faciale prometteur se vante d'utiliser une technologie IA avancée, offrant une précision et une rapidité comparables à celles de PimEyes. ■

FILADENDRON/ISTOCK; RISKA/ISTOCK

Vos courriels UNE AUBAINE POUR LES ESCROCS

En 2025, la boîte de réception est toujours la porte d'entrée préférée des pirates. Voici comment éviter de tomber dans leurs pièges.

À 8 h 17 ce matin, vous ouvrez votre messagerie avant de commencer votre journée. Un e-mail attire aussitôt votre attention: votre banque vous avertit d'une «activité suspecte» sur votre compte. Le logo est impeccable, le ton sérieux, et le lien vers «votre espace sécurisé» vous invite à agir immédiatement. Encore à moitié réveillé, vous cliquez. En moins de deux minutes, vos identifiants et votre mot de passe viennent de partir vers un serveur contrôlé par un pirate à l'autre bout du monde… Ce scénario n'a rien d'exceptionnel. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), le phishing demeure la menace numéro 1 en France, touchant aussi bien les particuliers, les PME que les grandes entreprises. Cybermalveillance.gouv.fr estime que les courriels sont toujours la principale porte d'entrée des cybermenaces, à 75 % – et ce chiffre reste stable malgré les campagnes de sensibilisation.

BACKCOUNTRY/ADOBE STOCK

SE PROTÉGER EFFICACEMENT

Si aucun remède miracle n'existe, un ensemble d'habitudes peut réduire drastiquement les risques de piratage via votre boîte mail. Ne livrez jamais d'informations sensibles par courriel ; vérifiez toujours l'expéditeur d'un message reçu et le lien qu'il contient avant de cliquer ; activez la double authentification sur vos comptes importants ; utilisez un antivirus et maintenez vos logiciels de messagerie à jour ; séparez vos usages (achats, administration, loisirs) en leur dédiant à chacun une adresse électronique spécifique.

DU PRINCE NIGÉRIAN À L'IA DE POINTE

Dans les années 2000, l'hameçonnage se repérait facilement: e-mails avec fautes d'orthographe grossières, histoires rocambolesques («héritage d'un prince africain»…), adresses électroniques improbables. En 2025, le décor a changé. Le phishing est passé d'attaques artisanales à de véritables industries criminelles structurées. Les malfrats ont désormais accès à des modèles professionnels copiés pixel par pixel depuis les vrais sites. LabHost, plateforme de phishing-as-a-service (PhaaS, ou «hameçonnage à la demande»), en est l'illustration parfaite. Avant sa fermeture par le FBI américain, ce site permettait à un pirate, même débutant, de planifier ses attaques. Ainsi, pour un abonnement d'environ 230 €, il pouvait déployer rapidement des sites frauduleux imitant plus de 170 banques, services publics et institutions; envoyer des e-mails ou des SMS piégés grâce à des modèles prêts à l'emploi; utiliser un outil de vol en temps réel des identifiants saisis par les victimes sur leur clavier… Démantelé en avril 2024 lors d'une opération internationale coordonnée par Europol, LabHost a laissé derrière lui 42 000 domaines malveillants répertoriés par les autorités. Cette affaire montre comment l'hameçonnage est devenu un service clés en main où la compétence technique n'est plus indispensable, ce qui en multiplie la portée et le danger à l'échelle mondiale.

DES DONNÉES VOLÉES POUR PERSONNALISER UN MESSAGE

Les outils d'IA générative rendent pratiquement n'importe qui capable d'écrire dans un style naturel, sans fautes, et d'imiter le ton d'un interlocuteur connu. L'attaquant ne se contente alors plus d'envoyer un lien frauduleux: il construit une expérience crédible de bout en bout, jusqu'à de faux numéros d'assistance téléphonique pour achever de tromper sa proie.

En avril 2024, une campagne massive d'e-mails imitant ceux envoyés par EDF a touché plusieurs dizaines de milliers de Français. Le message, visuellement parfait, avertissait d'une «facture impayée» et redirigeait vers un faux portail de règlement. Bilan: des centaines de victimes, et jusqu'à 4 000 € de pertes par personne. La gendarmerie a pu identifier un groupe criminel opérant depuis l'Europe de l'Est et l'arrêter, mais la plupart des fonds volés avaient déjà été blanchis.

OPÉRATION CACTUS
ÇA N'A PAS TROP PIQUÉ !

En mars 2025, la section cyber de la Juridiction nationale de lutte contre la criminalité organisée (Junalco), en partenariat avec les ministères de l'Éducation nationale et de l'Intérieur et les plateformes Cybermalveillance.gouv.fr et Cnil.fr, a lancé l'opération Cactus pour sensibiliser les jeunes aux dangers du phishing. Une simulation a ciblé 2,5 millions d'élèves: seuls 210 000 ont cliqué sur le lien problématique, soit 1 sur 12, ce qui montre que les jeunes ne sont pas si crédules face aux cyberattaques. Les espaces numériques de travail (ENT) scolaires, déjà touchés par une attaque massive en 2024, restent en première ligne en 2025.

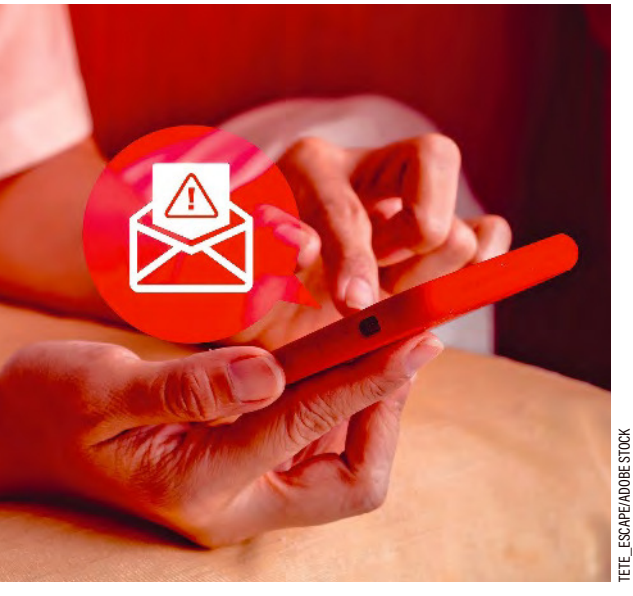
ADRESSE JETABLE POUR VISITE UNIQUE

L'adresse électronique jetable est une option intéressante quand vous devez vous inscrire sur un site que vous ne revisiterez sûrement pas. Ça tombe bien, de nombreux portails web en proposent d'éphémères. Vous ne souhaitez pas de redirection? Créez-vous un compte de messagerie sur YOPmail pour communiquer avec votre interlocuteur. Sa réponse sera lisible directement sur le site, qui fait office de boîte de réception. Attention, dans ce cas comme dans le précédent, vous n'êtes pas maître du stockage des informations. Par exemple, sur YOPmail, il suffit qu'une personne connaisse l'adresse électronique générée pour accéder à la boîte dédiée. Et alors, n'importe qui peut lire les contenus sauvegardés.

UN ALIAS CONSACRÉ AUX ACHATS

Vous utilisez la même adresse électronique pour vos achats en ligne, vos loisirs ou vos échanges avec l'Administration? Mais alors, tous vos œufs >>

>> sont dans le même panier, et si votre messagerie est corrompue, la gangrène s'étendra partout. Afin d'éviter cette situation, il est fortement conseillé de créer des «alias», c'est-à-dire des adresses secondaires. Accolés à la principale, ils comportent une signature distincte. Exemple: votre adresse habituelle est mail@operateur.fr. Pour le cinéma de quartier auquel vous êtes abonné, votre alias pourra ressembler à mailcinema@operateur.fr; pour votre association, à mailasso@operateur.fr; et ainsi de suite. Cela facilitera le classement de vos archives et ciblera parfaitement l'interlocuteur. Des solutions informatiques proposent de créer des alias gratuitement, comme SimpleLogin (Proton Mail) ou Firefox Relay (Mozilla).



TETE_ESCAPE/ADOBE STOCK

QUI SE CACHE DERRIÈRE L'ADRESSE ÉLECTRONIQUE ?

De multiples sites internet, publics ou payants, sont capables de trouver des informations sur l'émetteur d'une missive par l'intermédiaire de son adresse électronique. Parmi eux, le site Hunter.io/fr («chasseur») identifie gratuitement, en quelques secondes à peine, l'utilisateur d'un e-mail professionnel. Vous pourrez ainsi répondre rapidement à une question simple: «*Cette personne est-elle vraiment employée par l'entreprise qui me contacte ?*» Voyez votre messagerie comme une porte d'entrée; parfois, elle reste entrouverte sans que l'on s'en rende compte. La meilleure défense n'est alors pas un outil, mais une habitude: douter. Si un courriel vous demande d'agir en urgence, ralentissez. Si un lien vous semble correct, vérifiez-le quand même. Et même si tout paraît en ordre, méfiez-vous encore ! ■

6 BONNES PRATIQUES POUR UNE BOÎTE MAIL SÉCURISÉE

ASTUCES	POURQUOI C'EST IMPORTANT ?
Mettre à jour son logiciel de messagerie	**Permet de corriger** automatiquement les failles de sécurité connues (ex. Outlook, Thunderbird)
Activer les mises à jour automatiques	**Assure la protection** continue contre les vulnérabilités nouvellement découvertes
Désactiver l'aperçu automatique des messages	**Évite l'exécution** involontaire de code malveillant intégré à certains courriels
Interdire l'exécution d'ActiveX et de plug-in	**Empêche la propagation** de virus via des modules externes non sécurisés
Bloquer les téléchargements automatiques de pièces jointes	**Réduit le risque** d'infection par un logiciel malveillant caché dans un fichier
Lire les courriels en texte brut	**Neutralise les scripts** malveillants dissimulés dans des e-mails au format HTML

En voyage LA TO-DO LIST DE SÉCURITÉ

Bientôt le départ ? Soleil, détente… et prudence ! Un séjour réussi se mesure aussi à la sérénité avec laquelle vous rentrez.

Même en vacances, pas de repos pour la vigilance.

Avant même de boucler vos valises, créez une adresse mail spéciale vacances. Elle ne servira qu'à vos proches et aux hôtels ou guides sur place. Astuce: ajoutez un signe distinctif dans votre signature, comme un triple smiley, pour que vos contacts sachent qu'un message sans ce code n'est pas de vous. Profitez-en pour sauvegarder vos papiers d'identité et numéros utiles (ambassade, banque…) sur une clé USB, protégée par un mot de passe via 7-Zip (logiciel gratuit de compression de données). Glissez aussi dans vos affaires une pochette anti-NFC: elle empêchera la copie sans contact des données de votre carte bancaire ou de votre passeport. Avant de fermer la porte, coupez votre wifi domestique et activez la double authentification sur vos comptes, de préférence avec une clé physique ou une application plutôt qu'avec un simple SMS.

Évitez les connexions à vos comptes

Si vous allez à l'hôtel, ne perdez pas de vue la pièce d'identité confiée à la réception. Une copie en est faite ? Demandez à la vérifier et inscrivez-y la date et le nom de l'établissement. Durant votre séjour, fuyez les ordinateurs gratuits pour gérer vos affaires personnelles ou professionnelles. Si vous devez en utiliser un, effacez vos traces: écrasez le fichier avec un autre portant le même nom, rempli d'images ou de chiffres, et recommencez plusieurs fois. Anticipez vos impressions de documents: copiez-les sur votre clé USB avant de partir, afin de ne pas avoir à vous connecter à vos comptes à l'étranger. Car en voyage, et en particulier hors de France, mieux vaut éviter tout accès à des sites contenant vos données personnelles, et surtout jamais via une connexion à du wifi public. Si vous devez vraiment vous connecter, passez par un VPN, en gardant à l'esprit que certains pays les bloquent. Dernier conseil: ne mettez pas à jour vos appareils à l'étranger, vous empêcherez ainsi toute installation douteuse.

De retour à la maison, si vous avez accédé à vos comptes pendant le séjour, changez immédiatement vos mots de passe. Supprimez l'adresse électronique spéciale vacances pour qu'elle ne soit pas réutilisée. Enfin, remettez à jour vos appareils: ordinateur, tablette, smartphone, objets connectés… afin de clore votre voyage en toute sérénité. Dernier détail: votre messagerie doit être pleine. Prudence ! Un clic trop rapide sur un e-mail pour gagner du temps peut s'avérer fatal. ■

ASSURER SES ARRIÈRES

Utiliser un ordinateur public semble pratique, mais c'est dangereux. Un navigateur mal configuré stocke l'historique, les cookies et parfois les mots de passe. Le prochain visiteur peut accéder à vos messageries ou à vos réseaux sociaux rien qu'en ouvrant la page sur laquelle vous surfiez… Afin d'éviter tout risque, déconnectez-vous de vos comptes quand vous avez fini. Supprimez l'historique, les cookies et le contenu de la corbeille. Pour les fichiers téléchargés sensibles (billet d'avion…), écrasez l'original en en créant un volumineux du même nom. Et récupérez vos périphériques (clé USB) !

ANDRESR/ISTOCK

Sur le Web
LES PRÉCAUTIONS À PRENDRE

Nom, adresse, localisation… que vous le vouliez ou non, la Toile collecte des fragments de votre vie numérique. La bonne nouvelle ? Vous pouvez limiter ces fuites. La mauvaise ? Cela demande tout de même un peu de discipline.

Tout commence par un geste anodin: visiter un site, remplir un formulaire, s'inscrire à une newsletter… En quelques secondes, vous livrez des informations clés – nom, e-mail, numéro de téléphone –, mais aussi des données invisibles telles que votre géolocalisation, le système de votre appareil ou les réglages de votre navigateur. Et ce navigateur, justement, est votre première ligne de défense… ou votre pire ennemi. Chrome, Firefox, Safari, Edge, Opera, Brave, Vivaldi… chacun a ses atouts et ses faiblesses. Si Chrome séduit par sa vitesse et son intégration avec l'univers Google, Firefox, lui, plaît aux partisans de l'open source et de la personnalisation grâce à une riche bibliothèque d'extensions. Safari demeure l'allié des appareils Apple. Edge, bâti sur le même moteur que Chrome, offre un mode lecture et la gestion native de livres numériques. Opera propose un proxy (serveur distant) intégré au navigateur. Brave bloque les traqueurs publicitaires par défaut. À vous de choisir selon vos priorités: confort, rapidité ou confidentialité.

À ÉVITER

> **Se connecter** à ses comptes sensibles sur un wifi public sans protection VPN.

> **Réutiliser** le même mot de passe sur plusieurs sites.

> **Laisser le Bluetooth,** le wifi ou le NFC activés en permanence sur son smartphone.

> **Cliquer** sur un lien reçu par e-mail sans vérifier l'expéditeur et l'URL.

> **Télécharger** des extensions ou applications depuis des sources non officielles.

> **Négliger de mettre à jour** navigateur, système et antivirus.

> **Oublier ce point essentiel :** si c'est gratuit, ce sont vos données le produit.

NAVIGUER INCOGNITO

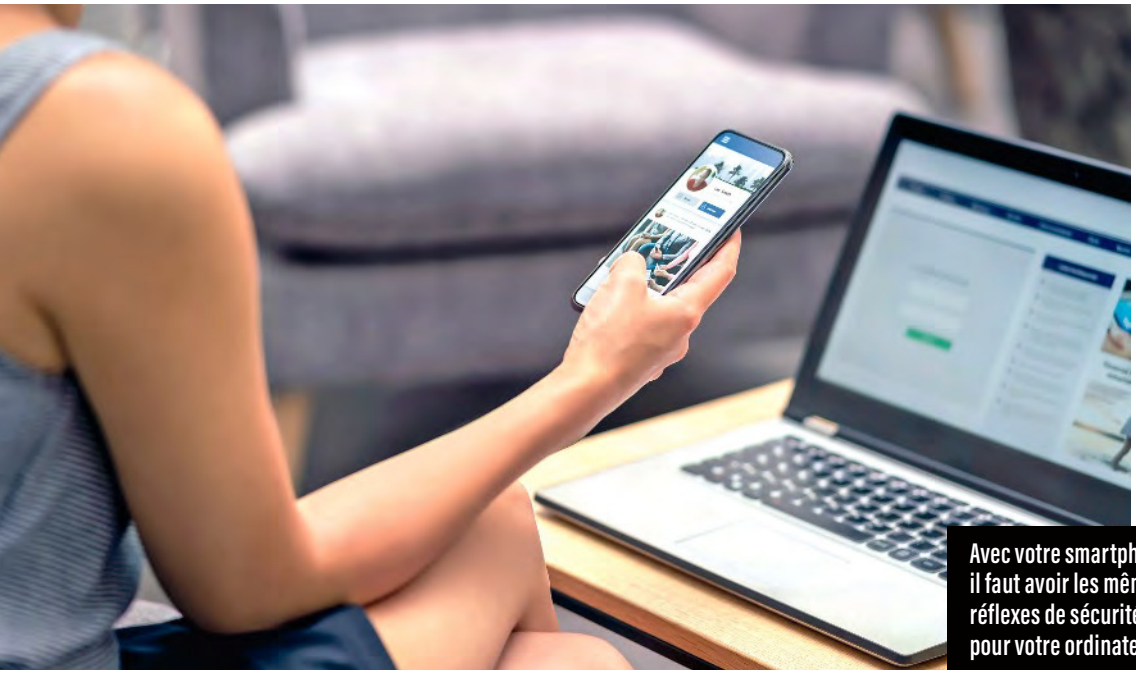
Tous les navigateurs proposent un mode de navigation privée. Pratique pour éviter que votre historique, vos cookies ou vos formulaires ne soient enregistrés. Cependant, attention, cela ne vous rend pas transparent: les sites visités, votre fournisseur d'accès, voire certaines autorités peuvent toujours voir vos connexions.

UN ESPION DE POCHE

Un téléphone moderne, c'est un ordinateur miniature et un collecteur de données redoutable (lire aussi p. 88). Avoir envers lui la même hygiène numérique qu'avec un PC s'impose, avec quelques précautions supplémentaires. Ainsi, coupez le wifi, le Bluetooth et le NFC lorsque vous ne les utilisez pas. Ces technologies servent parfois de porte d'entrée à des collectes non autorisées. Le NFC, par exemple, permet des échanges de données à très courte distance: idéal pour le paiement sans contact… mais aussi pour un transfert malveillant si vous êtes collé à un appareil compromis !

PROTECTION RAPPROCHÉE

Même les navigateurs les plus solides peuvent être «percés». Leurs mises à jour et celles de votre système d'exploitation sont indispensables, car elles



T. VESALAINEN/ISTOCK

Avec votre smartphone, il faut avoir les mêmes réflexes de sécurité que pour votre ordinateur.

colmatent les brèches dont les pirates profitent. Activez-les en mode automatique. Ajoutez-leur un antivirus fiable, et laissez-le se mettre à jour. Un antivirus obsolète, c'est une porte blindée… sans serrure.

DES EXTENSIONS QUI VOUS PROTÈGENT

Les navigateurs modernes offrent une mine d'extensions (petits modules logiciels permettant de les personnaliser) et de widgets (applis proposant d'ordinaire des informations ou des divertissements). Bien choisis, ils deviennent de super alliés. Ainsi, DNSlytics dévoile les dessous techniques d'un site (hébergeur, date de création, localisation); SimpleLogin sert à créer des adresses électroniques «alias» pour éviter de révéler la vôtre: en cas de fuite, vous n'avez qu'à supprimer l'alias compromis. La plupart des navigateurs proposent également un mode HTTPS unique. Il impose automatiquement la connexion chiffrée vers les sites compatibles et bloque les versions non sécurisées (sans le S) en HTTP.

VÉRIFIEZ AVANT DE CONFIER VOS DONNÉES

Avant de saisir un mot de passe ou vos coordonnées bancaires, jetez un œil à la barre d'adresse. Un petit cadenas accolé indique que l'on a affaire à une connexion chiffrée (HTTPS), toutefois il ne garantit pas que le site est digne de confiance. Des fraudeurs savent aussi afficher ce cadenas sur des pages piégées ! Enfin, souvenez-vous: un wifi public – celui du café, de l'hôtel ou de la gare – sert parfois de terrain de chasse aux malfaiteurs. Ce n'est pas parce qu'il est «offert par la direction» qu'il est sûr… En outre, certains lieux collectent légalement vos habitudes de navigation à des fins marketing. Pour consulter vos comptes bancaires ou envoyer des données sensibles, passez toujours par un VPN fiable. Nous vous conseillons d'utiliser directement le réseau mobile 4G/5G.

LE VRAI SECRET POUR RESTER DISCRET

La sécurité en ligne n'est pas qu'une affaire d'outils, c'est également une question de comportement. Limitez les inscriptions inutiles, évitez les clics impulsifs sur des liens douteux et paramétrez vos comptes afin de minimiser le partage d'informations. Enfin, régulièrement, prenez le temps de nettoyer votre historique et vos cookies. Naviguer sans se mettre à nu, c'est un peu comme voyager léger: vous gagnez en confort et laissez moins de traces derrière vous. ■

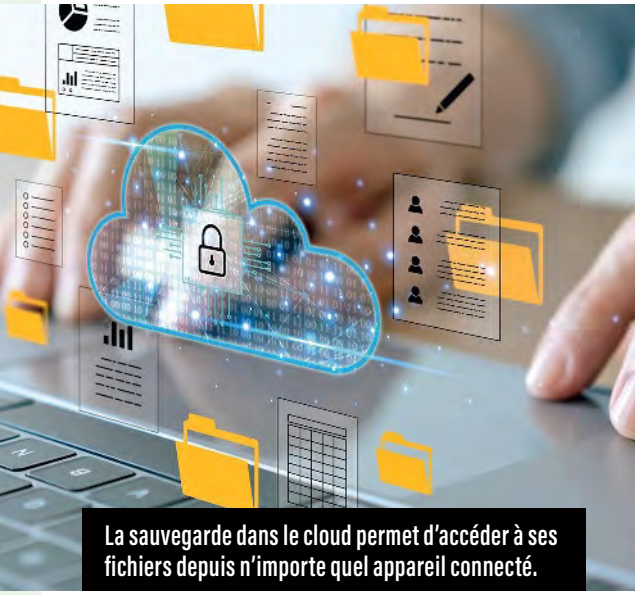
Sauvegarde en ligne

LE CLOUD, **SIMPLE ET PRATIQUE**

Nous avons testé 12 solutions de stockage de données en ligne, dont celles d'Apple, de Google et de Microsoft.

Une vie quotidienne dématérialisée exige quelques nouvelles habitudes de prudence. Votre ordinateur et votre smartphone sont devenus les points d'accès à vos documents administratifs (factures, avis d'imposition, courriers…), mais aussi à vos photos, vos contacts, vos échanges d'e-mails ou de textos. Avez-vous déjà imaginé tout perdre ? Panne, vol, casse, virus informatique… vos appareils sont vulnérables. Mettre ses données à l'abri est impératif. Ainsi, en cas de pépin, vous les retrouverez en deux clics.

La sauvegarde en ligne, dans le cloud, constitue une solution simple et pratique : vous accédez à vos fichiers depuis n'importe quel appareil connecté à Internet, et pouvez aussi les partager très facilement avec vos proches (des photos de vacances, par exemple). Enfin, et surtout, ces outils proposent une précieuse fonction de programmation de sauvegardes automatiques, ce qui assure de toujours disposer d'une copie de ses dossiers, même des plus récents.



La sauvegarde dans le cloud permet d'accéder à ses fichiers depuis n'importe quel appareil connecté.

KOTO AMASTUKAMI/ADOBE STOCK

Gratuites ou payantes ?

Les solutions de stockage sont nombreuses. Il y a d'abord celles d'Apple (iCloud), de Google (Drive) et de Microsoft (OneDrive), intégrées à votre environnement numérique si vous utilisez déjà un iPhone, un iPad ou un Mac, un PC sous Windows ou encore les services de Google. Libre à vous de vous en servir pour stocker vos documents. Vous pouvez, sinon, opter pour un logiciel alternatif (Dropbox, pCloud, kDrive, Icedrive, etc.). Pour ce test, nous en avons sélectionné 12, en choisissant uniquement des versions payantes qui comprennent de 500 Go à 2 To d'espace de stockage, car les 5 à 20 Go mis à disposition dans le cadre des offres gratuites ne suffisent pas.

Il est parfois possible de préférer une facturation au mois ou à l'année, cette dernière revenant un peu moins cher (deux mois gratuits, environ). Les outils pCloud et Internxt disposent même d'abonnements « à vie » : ils sont valables tant que vous êtes vivant… et ne dépassez pas l'âge de 99 ans (et à condition, bien sûr, que l'entreprise ne fasse pas faillite entre-temps). Les solutions cloud se déclinent en un logiciel à installer sur ordinateur et en une application à télécharger sur son smartphone ; l'utilisateur est ainsi en mesure de piloter ses fichiers depuis ces deux types d'appareils. Si Dropbox Plus s'avère la meilleure, elle est talonnée par plusieurs autres, dont Apple iCloud, Microsoft OneDrive ou pCloud Premium Plus. ■

Test

12 LOGICIELS DE SAUVEGARDE EN LIGNE

★★★ très bon
★★ bon ★ moyen
■ médiocre ■■ mauvais
● oui - non
n.a. : non applicable

		Performances – Windows (1)											Appréciation		
		Configuration	Sauvegarde	Synchronisation de fichiers	Accès aux données à distance	Partage de fichiers	Téléchargement	Vitesse de vitesse en écriture	Version macOS (2)	Application Android	Application iOS	Polyvalence	Note sur 20		Prix €/mois
1	**DROPBOX** PLUS	★★	★★★	★★★	★★★	★★★	★★★	★★★	★★★	★★	★★★	★★★	**16,5**	★★★	11,99
2	**APPLE** ICLOUD + 2 TO	★★★	★★	★★★	★★	★★★	★	■	★★	n.a.	★	★★★	**15,8**	★★	9,99
3	**MICROSOFT** ONEDRIVE	★★★	■■	★★★	★★★	★★★	■	■	★★	★★★	★★	★★★	**15,7**	★★	10
4	**PCLOUD** PREMIUM PLUS 2 TO	★★★	■■	★★	★★★	★★	★	★★★	★★	★★★	★★	★★★	**15,5**	★★	9,99 (3)
5	**IONOS** HIDRIVE NEXT PLUS 1 TO	★★★	■■	★★★	★★★	★★★	■■	■	★★	★★	★★★	★★★	**15,3**	★★	8,40
6	**MEGA** PRO I	★★	★★	★★★	★★★	★★	★★★	★★★	★★★	★	★	★★★	**15**	★★	11,99
7	**PROTON** DRIVE UNLIMITED 500 GO	★★★	■■	★★★	★★★	★★	■	■■	★★	★★★	★	★★★	**14,8**	★★	12,99
8	**INFOMANIAK** KDRIVE SOLO	★★	■■	★★★	★★★	★★★	■	■■	★★	★★★	■■	★★★	**13,8**	★★	5,54
9	**GOOGLE** DRIVE PREMIUM 2 TO	★★★	■■	★★★	★★★	★	★	★	★★	★★	■■	★★★	**13,4**	★★	9,99
10	**INTERNXT** ESSENTIEL	★★	★★★	★★★	★★★	★★★	■■	★	★★	■■	★★	★★	**12,8**	★★	18 (4)
11	**ICEDRIVE** PRO I	★	★★	★	★★★	★★★	■■	■■	★	★	★	★★★	**12,2**	★★	7,99
12	**TRESORIT** PERSONAL ESSENTIAL	★★	■■	★	★★	★★	■	■	★	■	★	★★	**11**	★	11,99

(1) Sur Mac OS pour iCloud.
(2) Version Windows pour iCloud.
(3) Ou 399 € à vie.
(4) Par an, ou 285 € à vie.

NOTRE MÉTHODE

Nous évaluons le fonctionnement (installation du logiciel, configuration, accès aux dossiers synchronisés, partage de fichiers, vitesses de transfert) sous Windows et sous MacOS. **Nous testons** aussi les applications Android et iOS (sauvegarde des photos et vidéos). Notre labo s'assure, enfin, de la présence des principales fonctionnalités attendues.

Le meilleur

Dropbox

Dropbox PLUS
11,99 €/mois **16,5/20** | ★★★

Avec cette version payante, Dropbox vous fournit 2 To de stockage en ligne (contre 2 Go pour la gratuite). De quoi consigner tous vos fichiers, auxquels vous accéderez depuis un ordinateur, un smartphone ou une tablette connectés. Simple à configurer, bien conçue en version Windows, MacOS et mobile (iOS, Android), cette solution est, de plus, très complète.

L'alternative

pCloud

pCloud PREMIUM PLUS
9,99 €/mois **15,5/20** | ★★

Une autre bonne alternative aux offres d'Apple, de Google et de Microsoft. Elle aussi permet le stockage, l'accès et le partage des fichiers de manière simple et sécurisée. Aucune difficulté de configuration ni d'utilisation ; le petit bémol vient de l'impossibilité de modifier des documents en ligne. Une version gratuite, avec 10 Go de stockage, est disponible.

Mini-guide *Sauvegarde en ligne*

STOCKER DANS LE CLOUD

Le cloud apporte la simplicité, grâce à des sauvegardes automatiques en arrière-plan, sans câble ni disque à brancher. Et il est facile de tout restaurer après la perte, le vol ou la casse du téléphone, de la tablette ou de l'ordinateur.

DES SERVEURS 100 % SÉCURISÉS EN FRANCE

Vos fichiers restent synchronisés entre vos appareils. La famille peut partager un espace et récupérer les photos sans jongler avec des clés USB. Les services «nuagiques» gèrent l'intégrité des données. Souvent inclus dans un abonnement, comme chez iCloud, Google One ou Microsoft 365, le coût est prévisible. Les photos sont dédupliquées, les vidéos, compressées, et l'espace s'optimise automatiquement. Vous souhaitez un stockage 100 % sécurisé ? Choisissez des hébergeurs français tels que OVH, Blue, Nuxit, o2switch, Gandi, etc.

CONTINUITÉ ET FLEXIBILITÉ

Pour un iPhone, iCloud sauvegarde automatiquement appareil, photos et messages. Sur Android, Google One et Google Photos offrent le même confort. Besoin de bureautique et d'un partage familial multiplateforme ? Microsoft OneDrive ou Google Drive restent simples. Il vous faut un coffre privé ? Étudiez les solutions des suisses Proton Drive et pCloud ou du canadien Sync.com, avec chiffrement côté client. Pour de gros volumes de photos, Google Photos, iCloud Photos et Amazon Photos optimisent l'espace, mais attention, le stockage n'est pas en France. Si vous avez un NAS[1], ajoutez une copie vers un cloud externe. Espace, prix, restauration, vitesse, historique illimité, client de sauvegarde, chiffrement, localisation des données et support sont les critères à prendre en compte. Astuce: gardez les photos dans deux services différents et testez la restauration mensuelle sur plusieurs machines, histoire d'être sûr de récupérer vos données.

ADOPTER LA RÈGLE 3-2-1 POUR PROTÉGER SES DONNÉES

Visez la règle 3-2-1: trois copies de vos données, soit deux sur des supports de stockage tels que disque dur interne/externe, serveur ou cloud et une hors site (par exemple, Dropbox, lire p. 41). Si possible, activez le chiffrement. Protégez le compte avec mot de passe long, gestionnaire, biométrie et double authentification quand vous le pouvez. Programmez une sauvegarde automatique hebdomadaire pour votre ordinateur. Testez une restauration chaque mois sur quelques fichiers afin de vérifier l'intégrité. Étiquetez les dossiers sensibles. Notez vos procédures dans un document accessible hors ligne. Il vous facilitera la récupération.

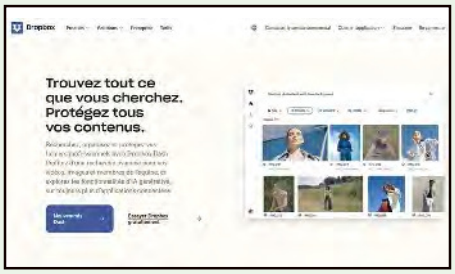
INCONVÉNIENTS À CONNAÎTRE

La confidentialité dépend des réglages et du fournisseur. Une mauvaise configuration risque d'exposer un dossier. Le coût de stockage grimpe avec les vidéos 4K, très lourdes. Certes rares, les pannes sont possibles. Un compte sans double authentification se pirate vite. Attention, certains services ne chiffrent pas de bout en bout par défaut. La localisation des données peut poser question selon la réglementation, alors mieux vaut sauvegarder en France. ■

(1) Dispositif de stockage de grande capacité connecté à un réseau.

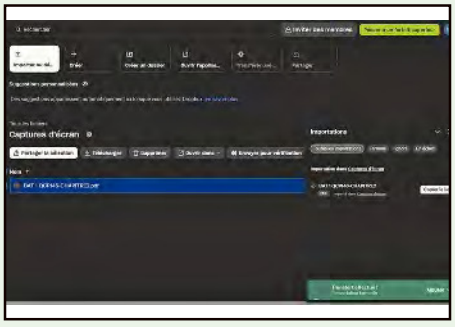
INSTALLER **DROPBOX**

Voici comment installer et configurer Dropbox, le meilleur des 12 logiciels de sauvegarde en ligne que nous avons testés (lire p. 39).



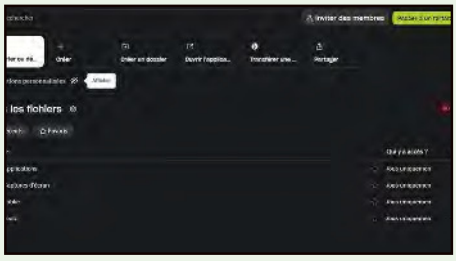
1 Rendez-vous sur Dropbox.com et créez un compte. Choisissez Windows, MacOS, Linux, iOS ou Android, puis installez le logiciel. La version gratuite se nomme Basic.

2 Ouvrez Dropbox et connectez-vous. Validez les autorisations. Choisissez le dossier local « Dropbox » pour la synchronisation avec vos fichiers.



3 Glissez-déposez un fichier dans « Dropbox ». Il se synchronise dans le cloud.

4 Accédez via l'application mobile ou web. Pour partager, faites un clic droit, puis « Partager », définissez les droits lecture/édition, copiez le lien.



5 Il est conseillé de créer des dossiers pour s'y retrouver. Activez « Smart Sync » ou « Selective Sync » afin de gagner de l'espace et d'automatiser les sauvegardes.

6 Activez la double authentification et vérifiez les appareils liés dans les paramètres, afin de vous assurer de ne sauvegarder que ce qui est autorisé.

Votre adresse IP
DIT TOUT DE VOUS…

Quand on souhaite demeurer anonyme sur Internet, la première chose à faire est de protéger son adresse IP, car elle peut permettre d'identifier indirectement une personne. Explications.

Certaines traces laissées sur le Web mènent jusqu'à un domicile, un ordinateur, voire directement à l'internaute. Dès lors, une personne qui veut rester anonyme doit supprimer ses traces du réseau, en commençant par son adresse Internet Protocol (IP). Celle-ci est constituée d'une série de nombres uniques identifiant un appareil connecté, qu'il s'agisse d'un ordinateur, d'un téléphone, d'une box ou d'une télévision. Chacun s'en voit attribuer une pour transmettre (recevoir et envoyer) des données. Sans trop entrer dans les détails, il en existe de deux sortes: IPv4 (version 4) et IPv6 (version 6). La première est composée de quatre nombres séparés par des points (par exemple, 192.168.0.1), et la seconde, de huit groupes de chiffres et de lettres séparés par deux points (par exemple, 2023:0db8:9282:9000:1111:8a2e:0370:1972). La masse d'équipements connectés grandissant de mois en mois, les adresses IPv6 ont été conçues pour que tous puissent en avoir une. Selon le Baromètre du numérique de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), en 2023, la France hébergeait environ 300 millions d'objets connectés. Le cabinet d'études américain IoT Analytics estimait, lui, leur nombre à 18,8 milliards dans le monde en 2024. Tous disposaient d'une adresse IP.

À QUOI ÇA SERT ?

Le protocole d'adressage Internet a plusieurs finalités. Outre l'identification des appareils qui se connectent à la Toile, l'IP sert à diriger (router) les données vers chaque demandeur. Ainsi, les informations sont envoyées à la bonne adresse, au bon serveur, à la bonne machine. D'ailleurs, sans cette adresse unique, impossible pour cette dernière de se connecter à un site web, à un réseau social ou à une webcam, ni de fournir les services en ligne demandés. L'IP est également utile au contrôle des connexions entrantes et sortantes d'un ordinateur. Certaines options sur les antivirus ou les systèmes d'exploitation assurent cette mission au moyen d'un outil baptisé firewall («porte coupe-feu»), qui bloque les connexions provenant d'adresses litigieuses (sites pornographiques, casinos, pirates, etc.). Parfois, l'IP analyse l'activité en ligne d'un usager afin de l'envoyer sur des pages dédiées à sa langue, sa localisation… C'est pourquoi la Commission nationale de l'informatique et des libertés (Cnil) considère que «*les adresses IP, qui permettent d'identifier indirectement une personne physique, constituent des données à caractère personnel dont la collecte relève d'un traitement de données nominatives devant faire l'objet d'une déclaration préalable auprès de la Cnil*». Ce protocole d'adressage entre, par conséquent, dans le cadre du Règlement général sur la protection des données personnelles (RGPD).

COMMENT PROTÉGER SON ADRESSE IP ?

Comme nous venons de le voir, éliminer l'IP de ses connexions internet est impossible. Il faut donc penser à une gestion réfléchie de cet élément d'identification. Ce qui semble le plus rapide et le plus facile, c'est d'utiliser un réseau privé virtuel (VPN), qui masque l'adresse IP de l'usager en la remplaçant par la sienne. Par exemple, l'IP «officielle» 192.168.0.1 apparaîtra sous l'adresse 123.45.67.8. Grâce à cette technique, on peut «faire croire» à un site situé au Canada que l'on est

La version 6 de l'Internet Protocol (IPv6) a été conçue pour répondre à l'augmentation exponentielle du nombre d'appareils connectés.

SATORI STUDIO/ADOBE STOCK

Canadien… Rappelons cependant que les éditeurs de VPN savent toujours, eux, qui l'on est vraiment. Et que les versions gratuites ne sont pas recommandées: en effet, lorsqu'un logiciel ou un service numérique ne coûte rien, c'est que la société qui le propose se rémunère avec les données de l'internaute qu'elle récolte. Par ailleurs, visiter des sites en HTTPS est indispensable, le «s» indiquant un chiffrement entre l'utilisateur et le site. Ajouter un VPN permet de cacher son identité au site consulté.

UN NAVIGATEUR DÉDIÉ

Pour protéger son adresse IP, on peut également installer un navigateur dédié. Le plus connu s'appelle Tor; il sait camoufler une véritable adresse IP avec celle d'un ordinateur hébergé dans un autre pays et exploitant le réseau Tor. Des applications pour navigateur, telles qu'uBlock Origin, permettent aussi d'empêcher les sites web visités par l'internaute de le géolocaliser à partir de son adresse IP. Enfin, il est important de ne jamais oublier que la sécurité et la protection à 100% n'existent pas. La sûreté numérique est un élément à concevoir sous la forme de «briques» à empiler. Par exemple, quand on veut surfer, il faut envisager l'usage d'un VPN et d'un antivirus, et se demander s'il est pertinent de fournir certaines données réclamées. ■

TROUVER MON ADRESSE ET MA VITESSE DE CONNEXION

Allez sur le site Adresseip.com. La page vous affichera la vôtre, ainsi que votre géolocalisation et le serveur utilisé pour router votre IP. Et si vous souhaitez connaître la vitesse de connexion de «votre» Internet, rendez-vous sur Fast.com.

Votre mobile COFFRE-FORT OU PASSOIRE ?

Votre smartphone embarque votre vie entière – identité, contacts, photos, historique de navigation… –, et cela intéresse autant les publicitaires que les cybercriminels. Voici comment protéger vos données.

Nos smartphones ont de plus en plus de risques de contenir une application malveillante; les protéger est donc essentiel. Les chiffres parlent d'eux-mêmes. Google annonce avoir bloqué 2,36 millions d'applis suspectes sur le Play Store d'Android en 2024. D'après le rapport de Kaspersky intitulé «Évolution des menaces informatiques au deuxième trimestre 2025: statistiques mobiles», rien que sur les six premiers mois de l'année, le nombre d'échantillons de logiciels malveillants détectés a atteint 180000, soit 29% de plus par rapport à la même période en 2024. Ces menaces ont été bloquées sur les smartphones Android de plus de 12 millions d'utilisateurs. Parmi les programmes malveillants les plus répandus, citons les chevaux de Troie bancaires, capables de vider un compte en quelques minutes, dont le nombre d'installations décelées a été multiplié par près de quatre en un an.

ILS ATTIRENT LES PIRATES

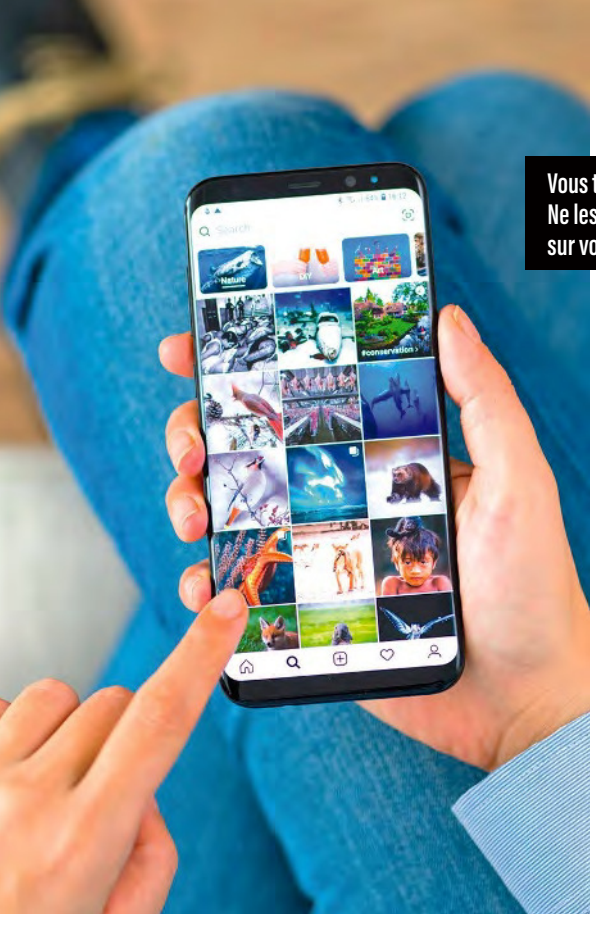
Il y a 20 ans, pirater l'ordinateur d'un particulier permettait déjà à un malfaiteur d'accéder à tous les documents personnels ou professionnels de sa proie. Aujourd'hui, votre smartphone concentre beaucoup plus d'informations précieuses sur vous: votre identité complète, vos coordonnées (numéros de téléphone, e-mails, carnet d'adresses), mais aussi vos photos, vos vidéos, vos fichiers privés, ainsi que vos codes d'accès à vos comptes en ligne (réseaux sociaux, banques, messageries…), sans oublier votre historique de navigation et votre géolocalisation. Par conséquent, pour un escroc, infiltrer un mobile, c'est disposer d'une porte d'entrée sur toute la vie numérique de sa victime. Ces données pourront être revendues sur des forums clandestins, utilisées pour usurper une identité ou comme monnaie d'échange contre une rançon.

EN 2025, DES MENACES PLUS DISCRÈTES ET PLUS CIBLÉES

Le malware (« logiciel malveillant ») visible, qui ralentissait le téléphone, appartient presque au passé. Désormais, les attaques sont invisibles: un lien frauduleux dans un SMS, une application téléchargée hors des boutiques officielles, un wifi piégé dans un café… Les chevaux de Troie bancaires ou les info-stealers («voleurs de données»), par exemple, affichent de fausses interfaces d'applis officielles pour subtiliser les identifiants et les codes bancaires des internautes. D'autres malwares interceptent les SMS contenant les codes de validation de paiements. Et le phénomène explose: le cybercrime mondial est estimé à 10,5 trillions de dollars en 2025 par le média spécialisé Cybersecurity Ventures (un trillion représente 1 000 milliards aux États-Unis et 1 milliard de milliards en France; ce que l'on

CONNAÎTRE LE NUMÉRO IMEI DE SON APPAREIL

Grâce à ce code, les opérateurs peuvent bloquer un téléphone signalé comme volé ou perdu, et ainsi empêcher qu'il soit utilisé sur leur réseau. Pour le connaître, tapez *#06# sur votre clavier (en lieu et place d'un numéro).



Vous tenez à vos photos ? Ne les stockez pas uniquement sur votre smartphone.

HOCU FOCUS/ISTOCK

CHECK-LIST EXPRESS DE LA SÉCURITÉ MOBILE

> **Verrouillage** Il se fait avec un mot de passe complexe (lettres, chiffres, symboles) ou une phrase de passe. Éviter le simple code PIN à quatre chiffres ; la biométrie est une option, mais toujours couplée à un mot de passe.

> **Authentification** Activer la double authentification (2FA) sur tous les comptes sensibles et utiliser un gestionnaire de mots de passe fiable.

> **Chiffrement et sécurité** Mettre en place le chiffrement natif du téléphone. Utiliser les « conteneurs sécurisés » ou espaces protégés ; noter et conserver le code Imei dans un endroit sûr.

> **Ce qu'il faut éviter** Stocker des infos bancaires ou codes sensibles en clair, garder toutes ses photos uniquement sur le mobile et se connecter à des wifis publics non sécurisés sans VPN.

> **Applications** Lire la politique de confidentialité avant toute installation. Révoquer les autorisations inutiles (caméra, localisation…), mettre à jour les applis régulièrement et supprimer celles inutilisées.

appelle trillion là-bas se nomme billion ici). Malgré tous les systèmes de sécurité déployés, la première ligne de défense contre les assauts des malfaiteurs demeure l'utilisateur.

BLINDER SON APPAREIL

Ce dernier doit, en premier lieu, veiller au verrouillage de son écran. Un code PIN simple à quatre chiffres est trop facile à casser, mieux vaut opter pour un mot de passe complexe (lettres, chiffres, caractères spéciaux), voire une phrase de passe (lire p. 47). La biométrie (empreinte digitale, reconnaissance faciale) est pratique, mais on privilégiera toujours, comme base, un mot de passe solide. Deuxième réflexe : l'activation de la double authentification (2FA) sur les comptes sensibles (messageries, réseaux sociaux, banque). Ce système, qui impose une deuxième preuve d'identité, rend les piratages bien plus difficiles. Le troisième geste consiste à mettre en place le chiffrement intégré du smartphone. Sur Android, certains modèles proposent des « conteneurs sécurisés » : des espaces invisibles et protégés, accessibles uniquement avec un mot de passe distinct. Enfin, connaître le code Imei de son smartphone (lire l'encadré p. 44) permet, en cas de vol, de demander à l'opérateur de bloquer l'appareil sur tous les réseaux.

CE QU'IL NE FAUT JAMAIS FAIRE

Stocker ses numéros de compte bancaire ou ses codes d'accès sur le téléphone est une erreur fréquente. Idem pour les photos et les vidéos : les garder seulement sur son mobile, sans sauvegarde externe, c'est risquer de tout perdre en cas de casse ou de vol. Mieux vaut effectuer régulièrement des sauvegardes sur un disque dur externe conservé chez soi. Pour le stockage dans le cloud, il faut vérifier dans quel pays se trouvent les serveurs de >>

>> ce dernier, et quelles lois s'y appliquent. Autre piège, se connecter à un wifi public inconnu, car ce type de réseaux peut avoir été falsifié de façon à intercepter les communications. Si l'on doit absolument y recourir, passer par un VPN (réseau privé virtuel) qui chiffre les échanges est indispensable. Rappelons que chaque application installée est un potentiel point d'entrée pour les malfrats. Avant de télécharger quoi que ce soit, on lira la politique de confidentialité: à quelles données la nouvelle appli aura-t-elle accès? Seront-elles chiffrées? Pourra-t-on demander leur suppression? Les boutiques officielles (Google Play, App Store) fournissent ces informations, mais elles sont modifiables à tout moment. Préférer les applis ayant subi un audit indépendant est une bonne pratique. Une fois qu'elles sont installées, il faut désactiver leurs autorisations inutiles (micro, caméra, géolocalisation…) et les mettre régulièrement à jour. Les nouvelles versions changent parfois les règles de collecte de données: lisez donc les notes de mise à jour… Enfin, et surtout, faites le ménage! Supprimez les applis inutilisées, cela réduit la surface d'attaque.

VCHALUP/ADOBE STOCK

MOTS DE PASSE À ÉVITER

> **Suites de chiffres** ou de lettres évidentes (1234, 0000, azerty);
> **Mots du dictionnaire,** même traduits;
> **Informations personnelles** (date de naissance, nom, ville);
> **Mots de passe déjà utilisés** sur d'autres comptes.

RISQUES ÉMERGENTS

Sur 2024-2025, le SIM *swapping* («piratage de carte SIM») est en hausse. Les pirates convainquent un opérateur de transférer un numéro vers une carte SIM en leur possession, puis interceptent les appels et les SMS qui lui sont adressés, y compris les codes 2FA. Autre tendance: l'hameçonnage via les messageries instantanées. Les messages frauduleux imitent des proches ou des services officiels et incitent à cliquer sur des liens infectés. Se faire passer pour un membre de la famille reste efficace…
On ne le dira jamais assez, la sécurité d'un smartphone n'est pas qu'une affaire de technologie, c'est aussi une question d'hygiène numérique. Verrouiller, chiffrer, sauvegarder, vérifier ses applis et éviter les réseaux douteux sont des gestes simples mais efficaces. À l'heure où un téléphone perdu ou compromis peut exposer toute une vie, rester maître de ses données n'a jamais été aussi vital!

LE MOT DE PASSE, PREMIER BOUCLIER

En 2025, un bon mot de passe vaut plus qu'un coffre rempli d'or. Il protège les comptes bancaires, les conversations privées, les souvenirs et même l'accès au travail. Pourtant, derrière ce simple assemblage de lettres, de chiffres et de symboles se cache souvent une faiblesse que les pirates savent exploiter. Selon une étude Google/The Harris Poll (2019), une large part des internautes emploient les mêmes mots de passe sur plusieurs comptes.
Des enquêtes sectorielles récentes (LastPass 2020, SpyCloud 2022, analyses 2024-2025) indiquent que 60 à 70% des utilisateurs reprennent des mots de passe, et les corpus de fuites montrent un taux de duplication encore plus élevé. Autrement dit, si un seul service en ligne est compromis, c'est tout l'écosystème numérique de l'internaute qui risque de tomber en quelques minutes. Imaginez: un pirate met la main sur votre mot de passe Netflix, fuitant lors d'une violation de données. En quelques secondes, il l'essaye sur votre boîte mail, vos réseaux sociaux, votre compte Amazon, et bingo!, il accède à tout. Ce phénomène, baptisé *credential stuffing* («bourrage d'identifiant»), est l'une des attaques les plus courantes. Et il ne nécessite aucune compétence technique avancée: un fichier de mots de passe volé et un logiciel automatisé suffisent.

PRÉVENTION/RÉACTION QUE FAIRE EN CAS DE PERTE OU DE VOL

QUAND	ACTIONS	DÉTAILS
AVANT	**Protéger l'accès au téléphone**	Un mot de passe fort. Faire de même pour la carte microSD
	Sécuriser la carte SIM	Changer le code PIN (éviter « 0000 », dates, etc.)
	Noter le numéro IMEI	Code unique à 15 chiffres, utile pour bloquer l'appareil. Trouvable sur la batterie, l'emballage ou en tapant *#06#
	Activer la géolocalisation	Permet de retrouver l'appareil ou de l'effacer à distance
	Activer le blocage/effacement à distance	Option souvent présente dans les réglages de sécurité
APRÈS	**Changer tous les mots de passe**	Messagerie, comptes en ligne, boutique d'applis, banque, etc.
	Prévenir l'opérateur	Demander le blocage de la carte SIM
	Déposer plainte	Au commissariat ou à la gendarmerie, avec le numéro IMEI

UN CONFORT QUI COÛTE CHER

Face à la multiplication des comptes en ligne – 197,5 par personne, en moyenne, actuellement selon les professionnels du secteur –, beaucoup d'internautes optent pour la facilité (lire également l'encadré «Mots de passe à éviter» p. 46). On choisit un mot de passe simple à retenir: «azerty», «123456», le prénom de son enfant ou celui du chat. Parfois, on complexifie un peu, mais pas assez… «Azerty2025» ou «Loulou75» ne résisteront pas plus d'une seconde face à un logiciel de *brute force* (spécialisé en cassage de codes). La réalité est là: les pirates disposent aujourd'hui d'outils capables de tester des milliards de combinaisons à la seconde. Avec un mot de passe court et prévisible, la partie est perdue avant même d'avoir commencé.

LA PHRASE, UNE BONNE IDÉE… À RÉINVENTER

Depuis quelques années, les experts en sécurité recommandent la phrase de passe: une phrase entière, parfois tirée d'un livre, d'un film ou d'une chanson. L'avantage? Elle est longue, donc plus difficile à casser, et s'avère plus facile à retenir qu'une suite aléatoire de caractères. Voici un exemple, mais à vous d'inventer les vôtres… Dans *L'art de la guerre,* de Sun Tzu (écrit au V^e^ siècle avant J.-C.), choisissons la phrase *«Connais ton ennemi et connais-toi toi-même, et tu pourras livrer cent batailles sans jamais être en danger.»* Prenons les lettres initiales de chaque mot: C t e e c t t m e t p l c b s j ê e d. On évite les substitutions trop connues (o = 0, ou e = 3), afin de déjouer les attaques par dictionnaire, et on remplace la lettre t par le symbole † (croix) et le e par €. Puis on ajoute le nombre de lettres dans chaque mot (connais = c7) et des majuscules pour certaines initiales. Ce qui peut donner, in fine, le mot de passe suivant: c7†3€6€2†7†3†3m4G6€2†2P7L6C4B9S4j6Ê4E2d6. Dans tous les cas, il faut utiliser un symbole inhabituel († ou §) au lieu des classiques (! ou @), et cacher un mot-clé secret dans la séquence (ici, G6) pour vous en souvenir. Enfin et toujours, on ne réutilise pas ce mot de passe, même modifié, sur plusieurs comptes ! ■

Vos réseaux sociaux
SÉCURISEZ WHATSAPP

Cette messagerie s'est rendue indispensable partout dans le monde. Découvrez comment l'utiliser en protégeant vos échanges.

WhatsApp propose désormais une fonction «Vue unique» pour envoyer des messages photos, vidéos ou vocaux qui disparaissent de la conversation après ouverture. Idéale pour partager des éléments sensibles (RIB…), elle empêche tout enregistrement, transfert ou capture d'écran par le destinataire (mais non la capture via un autre appareil). La plateforme offre aussi des outils de confidentialité: blocage de contacts, paramétrage fin des informations visibles, signalement de contenus problématiques et protection contre les messages indésirables.

Photo, vidéo ou vocal à vue unique

Ouvrez une discussion individuelle ou de groupe. Appuyez sur «Joindre» (le signe +), puis choisissez «Caméra» si vous souhaitez prendre une photo ou filmer, ou «Galerie» s'il s'agit de sélectionner un fichier existant. Activez la vue unique en touchant l'icône dédiée (chiffre 1 dans un cercle partiellement en pointillé). Lorsqu'il devient vert, le mode est actif, vous pouvez appuyer sur «Envoyer» (avion en papier). Votre destinataire ne pourra ni transférer, ni copier le message (pas de sauvegarde possible dans sa galerie ou ses photos), ni effectuer de capture d'écran. Toutefois, rien n'empêche qu'il photographie l'écran avec un autre appareil… WhatsApp applique le même principe aux messages vocaux: vous pouvez envoyer un enregistrement qui ne sera écouté qu'une seule fois avant de s'effacer. Pour cela, ouvrez une discussion, appuyez sur le micro et faites glisser vers le haut afin de lancer le mode mains libres. Activez la vue unique (chiffre 1 cerclé de pointillés). Quand l'icône est verte, enregistrez puis envoyez. Si le destinataire a autorisé les confirmations de lecture, votre message sera marqué «ouvert» dès sa consultation, sinon il disparaîtra sans indication visible.

En outre, WhatsApp propose une protection avancée via ses réglages. Par défaut, vos paramètres autorisent tout le monde à voir votre photo de profil et à savoir si vous êtes en ligne. Ils permettent aussi à vos contacts de voir votre statut et votre dernière connexion, et à n'importe qui d'ajouter des personnes dans des groupes. Mais vous avez la possibilité de modifier tout cela dans le menu «Confidentialité» afin de limiter l'exposition de vos données. Vous pourrez également activer les fonctions blocage et signalement pour couper toute interaction avec un contact indésirable; le filtrage des numéros inconnus, afin de détecter l'origine et les éventuels groupes communs avant réponse; la protection contre les spams, pour bloquer (avec plus ou moins de réussite) les envois massifs par des comptes inconnus; le partage de localisation sécurisé, de façon à n'informer de votre position que des personnes de confiance. Dans tous les cas, demeurez vigilant avant d'envoyer un message. Demandez-vous toujours si vous êtes prêt à en voir le contenu circuler publiquement. ■

ALEKSEI/ADOBE STOCK

Ne gardez pas les réglages par défaut de WhatsApp, utilisez son menu « Confidentialité ».

FACEBOOK IS WATCHING YOU ! *

Le réseau social le plus connu au monde détient des milliards de données personnelles sur ses utilisateurs. On vous explique comment garder le contrôle.

Facebook compte plus de 3 milliards d'utilisateurs dans le monde.

GUTEKSK7/ISTOCK; ROSSHELEN/ISTOCK

Université de Harvard, États-Unis, 2004. Plusieurs étudiants en informatique, dont Mark Zuckerberg, veulent lancer un réseau social pour communiquer et rester en contact avec leurs camarades. Ils inventent The Facebook, dont le succès dépasse rapidement leur campus pour s'inviter dans des dizaines d'universités américaines, puis bien au-delà… En 2025, avec 31,5 millions d'utilisateurs en France et plus de 3 milliards dans le monde (chiffres 2024), ce réseau social du groupe Meta est un géant du stockage de données personnelles. Mais tous ses usagers en sont-ils bien informés ? Si vous avez un compte Facebook, vérifiez souvent vos paramètres de confidentialité (vous y accédez en cliquant sur la flèche vers le bas, en haut à droite de votre page). Assurez-vous que votre profil est privé et que seuls vos amis voient vos publications. Vous pouvez aussi restreindre l'accès à certains renseignements tels votre date de naissance, votre adresse e-mail ou votre numéro de téléphone. Jetez régulièrement un œil sur les règles, car Facebook, lors de ses mises à jour, peut décider d'ajouter ou de retirer des paramètres. Ainsi, en février 2023, Meta a rendu payante la possibilité de recevoir par SMS le code de double authentification (2FA) qui permet d'accéder à son espace de réseautage en toute sécurité…

BIEN PROTÉGER SON COMPTE

Le mot de passe constitue la première ligne de défense de votre compte Facebook – autrement dit, d'une foule d'informations sensibles concernant votre vie privée. Alors, ne le négligez surtout pas ! Comme vous avez déjà pu le lire auparavant (p. 46-47), afin qu'il soit suffisamment fort, il faut impérativement mixer les chiffres, les lettres et les signes de ponctuation. En tant qu'utilisateur, vous avez également tout intérêt à opter pour l'authentification à deux facteurs, car même si la version SMS est devenue payante, il demeure possible de recevoir son code 2FA >>

>> via son application téléphonique ou des outils dédiés (comme Proton Authenticator, Authy, YubiKey… présentés p. 25). Vous pouvez la configurer en cliquant sur « Paramètres et confidentialité > Sécurité et connexion > Utiliser l'authentification à deux facteurs ».

SE GARDER DES FAUX AMIS

Le côté positif du réseau, c'est qu'il permet de retrouver des proches et des amis perdus de vue, et aussi de faire connaissance avec des inconnus ayant les mêmes centres d'intérêt. Cependant, et d'autant plus sur Facebook, gardez votre bon sens en alerte. Fuyez les demandes de personnes que vous ne connaissez pas. Les escrocs pullulent et peuvent recourir à de faux comptes afin d'accéder à vos informations personnelles. Il est également important de signaler ceux qui vous paraissent suspects. Pour avoir une idée de la menace, sachez que Meta a détruit des milliards de faux comptes sur sa plateforme Facebook depuis janvier 2019. D'ailleurs, celle-ci disposerait de 15 000 modérateurs; X emploierait 2 294 personnes dédiées à la modération; TikTok, 6 125; Snapchat, 2 198. Il en va de même pour les applications que vous autorisez sur votre page Facebook: évitez ces jeux ou ces questionnaires amusants au premier abord, mais qui ne sont rien d'autre que des collecteurs d'informations personnelles. Vérifiez les paramètres de confidentialité de ces applications tierces, et interdisez-leur l'accès aux renseignements que vous ne souhaitez pas partager. Bref, ne téléchargez que ce dont vous avez vraiment besoin, et effacez le reste !

VÉRIFIEZ LES DONNÉES RÉSIDUELLES

Si vous fermez vos comptes (lire aussi l'encadré p. 27), attendez trois mois puis tapez votre nom/pseudonyme sur Google et sur le moteur de recherche interne de Facebook/Instagram. Vous ne devriez plus apparaître. Dans le cas contraire, utilisez le droit à l'oubli (lire aussi p. 15) garanti par le Règlement général sur la protection des données (RGPD). De même si des informations persistent sur des comptes tiers ou dans des archives publiques.

VEILLER À CE QUE L'ON PUBLIE, PARTAGE, AIME…

Quand vous postez des photos sur votre page, êtes-vous attentif aux arrière-plans ? Aux reflets dans le miroir ? Ils peuvent en dire long. Vérifiez

N'interagissez pas trop. Vos likes et vos commentaires en disent beaucoup sur vous…

URUPONG/ISTOCK

les paramètres de confidentialité de vos publications, assurez-vous que seules les personnes autorisées (les amis) y ont accès, et qu'il n'est pas possible de les repartager. Il en va de même avec les «J'aime» («Like») et les autres commentaires que vous laissez. Attention, d'aucuns sont susceptibles de les utiliser afin de vous retrouver et de remonter ensuite toute votre vie numérique sur Facebook… À ce propos, regardez bien comment les internautes ont les moyens d'accéder à votre page. Pour cela, contrôlez qui peut vous voir (toujours dans l'espace d'administration de votre compte) en agissant sur les paramètres de confidentialité de la recherche, mais également qui est en mesure de vous envoyer des demandes d'amis ou des messages. Et c'est pareil avec les liens reçus sur Facebook et Messenger (le système de messagerie instantanée du réseau social): il vous faut les paramétrer.

SE PROTÉGER DE LA PUB ?

Sachez que Meta investit actuellement énormément d'argent et recrute massivement afin de créer des assistants personnels basés sur l'intelligence artificielle. À cette fin, elle installe des infrastructures informatiques très puissantes. Les étapes prévues incluent le déploiement de super-clusters (d'énormes ensembles de serveurs conçus pour entraîner des modèles d'IA à grande échelle) en 2026, et le développement de modèles de langage (*large language models,* ou LLM) encore plus puissants, au sein de son unité de recherche appelée TBD Lab. Bref, l'IA débarque en force sur Facebook et Instagram. Du point de vue de l'utilisateur, cela devrait signifier des outils intégrés plus performants, tandis que du côté des professionnels du marketing, on se prépare à l'automatisation généralisée des campagnes de publicité. Il va être très difficile de s'en protéger…

ACTIVER LES RESTRICTIONS

Même si Meta vous demande une autorisation de ne pas vous espionner (au lieu d'une autorisation à collecter), limitez les informations que vous lui donnez (adresse précise, date de naissance complète, informations familiales). Configurez les paramètres de confidentialité avec restriction sur vos publications, votre photo de profil et vos likes. Empêchez l'indexation dans les moteurs de recherche (option: gestion de votre compte). Vérifiez la section «Activité en dehors de Facebook» et supprimez l'historique. Désactivez l'analyse automatique des photos et vidéos, cela empêche l'IA de Meta de taguer les visages ou les objets. Cette dernière apprend énormément via vos «likes», vos temps de lecture et vos partages, alors si vous souhaitez limiter le profilage comportemental, interagissez moins avec les contenus, ou de façon aléatoire pour brouiller le profil. Si vous n'avez pas répondu à l'«avertissement» de Meta en juin 2025, toutes vos données préalables ont été «servies» à l'IA. Aujourd'hui, quand vous publiez des images, ajoutez discrètement un *watermark* (même léger) afin d'éviter qu'elles ne soient employées par des IA génératives: vos initiales, une fleur, etc. Dernier point: n'utilisez pas des services tiers via «Se connecter avec Facebook», car cela partage plus de données. ■

**Facebook vous regarde !*

VOTRE «HISTOIRE» FACEBOOK

Vous souhaitez savoir tout ce qui a été diffusé sur Facebook vous concernant? Connectez-vous à votre compte, cliquez sur l'icône en forme de flèche dans le coin supérieur droit de la page d'accueil, et sélectionnez, dans le menu déroulant, «Activité de recherche». Toutes les recherches que vous avez effectuées depuis la création de votre compte s'affichent alors, par ordre chronologique. Pour en supprimer une, survolez-la avec votre curseur et cliquez sur «Supprimer», à droite. S'agissant de l'historique de votre parcours, sélectionnez «Paramètres et confidentialité > Paramètres». Puis, dans le menu de gauche, «Vos informations Facebook». Cliquez sur «Télécharger vos informations»: une liste de catégories d'informations à télécharger apparaît. Cochez celles que vous désirez recevoir. Il est également possible de définir une plage de dates. Il faut ensuite un certain temps pour que les fichiers soient générés. Lorsque cette archive est prête (il arrive qu'elle soit très lourde), une notification vous invite à la télécharger. Pour en savoir plus, allez sur Facebook.com/help.


CARTE BLEUE
VISA
MR JEAN CARD
EXPIRE
A FIN
02/0
4942 9201 7913

Éviter les arnaques

L'inventivité des cybercriminels est sans limites. La diversité de leurs méthodes et la violence de leurs attaques également. Les chiffres 2024 de Cybermalveillance.gouv.fr le confirment: en France, l'hameçonnage (près de 34% des signalements) est en hausse de 23% en un an; le piratage de comptes progresse de 47%; les violations de données personnelles grimpent de 82%. Quant aux fraudes au virement, elles explosent: +603% chez les particuliers. Plus largement, les bonds faits par les malwares (+58%), les spams (+54%), le cyberharcèlement (+31%) et la fraude au faux conseiller bancaire (+18%) traduisent une intensification alarmante des pièges… Voici des pistes pour les déjouer.

SOMMAIRE

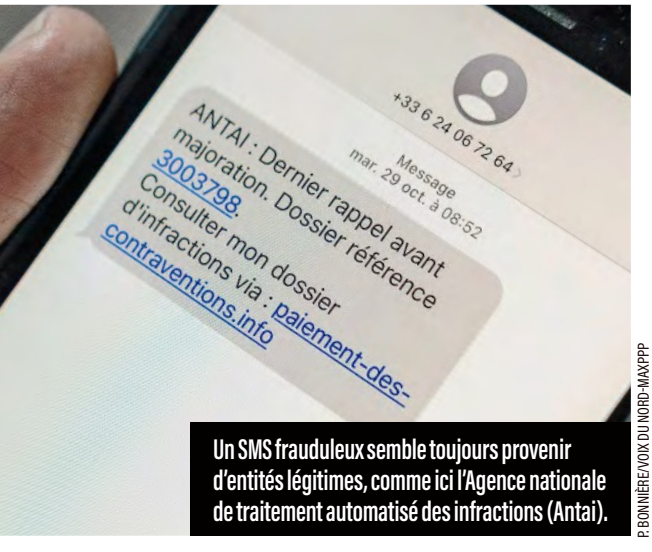
EXENTIVA/ADOBE STOCK ; KUNST-MP/ISTOCK ; C. ABAD/PHOTONONSTOP

LES PIÈGES COURANTS

Parmi les différents types de cyberattaques, certaines sont plus fréquentes que d'autres. En voici quelques-unes que vous trouverez sûrement sur votre chemin numérique un jour ou l'autre.

HAMEÇONNAGE (PHISHING)

Ce mode de piratage passe par des courriers électroniques, des SMS, des appels téléphoniques qui semblent provenir d'entités légitimes comme votre banque, un site de commerce en ligne ou encore l'administration fiscale. Le but est de vous inciter à fournir des informations personnelles sensibles telles que vos mots de passe, numéros de cartes de crédit ou informations d'assuré social. Attention, le phishing peut se faire via des accès entreprise que, normalement, seuls les employés connaissent et utilisent.



Un SMS frauduleux semble toujours provenir d'entités légitimes, comme ici l'Agence nationale de traitement automatisé des infractions (Antai).

P. BONNIÈRE/VOIX DU NORD-MAXPPP

Bon à savoir

Chasseurs de fausses URL

Plusieurs sites, dont Red Flag Domains ou PhishTank, répertorient les adresses de sites malveillants acquises par des pirates, soit plusieurs centaines par mois !

ADRESSES URL PIÉGÉES

Derrière un hameçonnage se cache aussi, de plus en plus souvent, un site web malveillant, usurpant le nom d'une société réelle ou modifiant légèrement son URL officielle. Dans un premier cas, les escrocs pratiquent le *typosquatting*. Cette technique consiste à enregistrer des noms de domaine qui ressemblent fortement à ceux de marques ou de sites connus, mais avec une orthographe légèrement différente, ou en remplaçant des lettres. L'idée est de profiter des erreurs de frappe courantes des internautes qui tapent l'URL dans leur navigateur pour les diriger vers des sites frauduleux ou les amener à divulguer des informations sensibles. Car, à la lecture, surtout via un smartphone, les usagers peuvent ne pas remarquer la légère modification… Illustration avec un des cas les plus marquants de ces dernières années, celui concernant l'adresse de l'Assurance maladie (Ameli.fr). Des escrocs avaient découvert que, dans un SMS, un «I» majuscule ressemblait beaucoup à un «l» minuscule. Ils avaient donc acheté le nom de domaine AMEIi.fr (Ameii.fr)… La technique de l'enregistrement d'un nom de site proche, mais avec quelques lettres modifiées, est également fréquente (Chrronopost.fr, Netfliix.fr, Vignettes-airgouv.fr…). Autre cas possible (et il en existe encore beaucoup): la création d'un nom de domaine qui n'appartient pas à l'entreprise, le pirate y ajoutant des mots. Par exemple, le nom de la Commission nationale de l'informatique et des libertés a été intégré dans l'URL du faux site «Sanctions-cnil.fr».

PETITES ANNONCES DÉGUISÉES

Une maison à vendre qui n'existe pas; une offre d'emploi qui devient une collecte de données d'entreprises pour lesquelles vous avez travaillé

KUPPA_ROCK/ISTOCK ; NEW AFRICA/ADOBE STOCK

Vous venez soi-disant de gagner un téléphone dernier cri sans avoir participé au moindre jeu ? Attention, il s'agit d'une arnaque à la loterie.

dans le passé, une rencontre amoureuse qui se transforme en prélèvements sur votre compte en banque… les fausses petites annonces pullulent et ciblent tous les secteurs. Voici quatre exemples emblématiques.

> **L'arnaque au chaton** Un particulier publie sur Facebook la photographie d'adorables petits chats et indique qu'ils sont à donner. Il n'a pas les moyens de s'en charger et recherche des âmes charitables. Son premier contact avec les candidats à l'adoption est évidemment chaleureux, il leur assure que la boule de poils leur sera livrée à domicile dans les 48 heures. Or, le lendemain, ils reçoivent un courriel d'un «vétérinaire» travaillant pour une société de transport d'animaux, qui leur dit que Minou a besoin d'une cage spéciale ou d'un vaccin. Le coût ? Entre 80 et 250 €. Une page de transaction est envoyée pour le paiement. Toutefois, le matou, lui, n'arrive jamais, car il n'existe pas ! En plus de l'argent de ses victimes, l'escroc aura collecté leurs données personnelles et celles de leur carte bancaire.

> **Le placement à trop beaux rendements** Cette arnaque consiste à inciter les gens à investir leur argent dans des entreprises fictives ou des projets qui ne sont pas rentables. Les cryptomonnaies ont favorisé ce type de piège. Dites-le-vous une bonne fois pour toutes: les rendements de 25, 50, voire 100 %, c'est trop beau pour être vrai !

> **L'arnaque à la loterie** Incroyable, quelle chance, vous venez de gagner un téléphone dernier cri ! Ne vous reste plus qu'à payer des frais de livraison pour «obtenir» votre cadeau…

> **Le chantage** Vous avez reçu des messages intimidants, du genre «Je t'ai vu via ta webcam» ou «J'ai piraté ton PC»? Depuis quatre ans, ces tentatives d'extorsions explosent. Les cybercriminels écrivent à des centaines de milliers de personnes dont, en réalité, ils ne savent rien; l'idée est de leur faire peur. La missive malveillante leur annonce le piratage de leur ordinateur et l'exfiltration de données «compromettantes». En échange de >>

>> son silence, le malfrat réclame quelques centaines d'euros. C'est du bluff, il n'a rien infiltré. Mais l'affolement pousse certains particuliers à payer.

> La star et la cryptomonnaie Des escrocs exploitent l'image d'artistes pour piéger des particuliers sur Facebook, avant de les rediriger vers la messagerie Telegram. En France, en 2025, ils se sont fait passer pour le chanteur Julien Doré (ou son manager) afin d'inspirer confiance aux proies. L'arnaque joue sur l'émotion et les promesses: rencontres VIP, projets caritatifs, investissements en cryptomonnaie… Les victimes, souvent des gens fragiles ou des fans inconditionnels, sont incitées à envoyer de l'argent, parfois des centaines d'euros, convaincues d'aider ou de bénéficier de gains.

BLOG RELAYANT UN LIEN MALVEILLANT

Vous avez un blog sur lequel vous partagez vos passions et vos centres d'intérêt. Il vous arrive d'y diffuser des liens vers d'autres espaces numériques. Un jour, vous recevez le courriel d'un inconnu qui vous explique que votre dernier post est génial, mais que l'adresse web indiquée n'est plus valide, qu'elle n'a pas été mise à jour. Il vous en propose une autre à la place. Ne l'acceptez surtout pas ! Il peut s'agir d'un lien malveillant (vers un casino, un site de contrefaçons, etc.), que le pirate activera quelques semaines plus tard. Il ne cherche qu'à profiter de votre blog et du référencement de celui-ci pour attirer les crédules dans son piège.

INFILTRATION DANS L'ESPACE PRIVÉ

En pénétrant vos espaces numériques (commerce, impôts, banque, etc.), les pirates ne vont pas obligatoirement vous voler directement. Ils peuvent conserver vos données et s'en servir plus tard, afin de détourner une somme, comme c'est parfois le cas avec le Trésor. Ainsi, par le biais d'un phishing, entre autres, le malfaiteur réussit à prendre la main sur votre espace personnel sur le site des impôts. Il modifie les montants déclarés, en y ajoutant, par exemple, des dons à des associations caritatives, l'emploi d'une nounou, d'un jardinier… Son idée ? Profiter du dégrèvement

La cryptomonnaie a favorisé l'essor d'offres d'investissement mirobolantes. Mais un rendement de 100 %, ça n'existe pas !

WRIGHTSTUDIO/ADOBE STOCK

fiscal et récupérer le remboursement de l'administration. L'argent lui sera envoyé par lettre chèque à l'adresse modifiée à cet effet, ou versé sur un compte bancaire ouvert pour l'occasion.

DOCUMENTS EXIGÉS POUR UN LOGEMENT

Vous êtes en quête d'un bien à louer, et une petite annonce attire votre attention. Votre interlocuteur, que vous avez contacté par téléphone et par e-mail, semble fiable et sérieux. Une fois la confiance installée, il vous réclame un certain nombre de pièces pour l'appartement que vous convoitez. Surtout, n'envoyez rien par courriel ! Cet aimable propriétaire pourrait bien être un escroc. Son unique objectif ? Vous soutirer un maximum d'informations personnelles afin de s'en servir ensuite (dans le but d'usurper votre identité, entre autres). Sachez que les pouvoirs publics donnent aux candidats locataires la possibilité de fournir les documents exigés de façon sécurisée. Leur site, Dossierfacile.logement.gouv.fr (vérifiez bien la présence de l'extension .gouv.fr, car des pirates ont créé des imitations), permet de déposer les justificatifs destinés au bailleur, lequel doit également posséder un compte pour les consulter, ce qui limite grandement les fraudes et facilite les démarches. Attention ! Ce dernier ne peut vous demander que les pièces dûment autorisées (détaillées sur Service-public.fr/particuliers/vosdroits/F1169), sans quoi il encourt 3 000 € d'amende (et 15 000 € pour une personne morale). À noter : si une copie de pièce d'identité lui est fournie en noir et blanc, en basse définition ou barrée, il a le droit de réclamer la présentation de l'originale.

FAUX COURS PARTICULIERS

En octobre 2022, la Direction générale de la sécurité intérieure (DGSI) alerte sur des cours particuliers… très particuliers. Des étudiants sont approchés par des individus souhaitant des leçons de mathématiques, d'économie, etc., contre paiement. Les cours ont bien lieu, la confiance s'installe. Mais, petit à petit, l'élève pose à son professeur des questions sur son emploi, ses activités… En réalité, il s'agit d'infiltrations menées par des agents des services secrets russes. Le contre-espionnage français met en garde : « *Progressivement, votre "élève" dévie du sujet […]. Il sollicite votre concours pour l'aider à rédiger des notes d'analyse ou de synthèse sur des thèmes touchant votre champ de compétence,* explique la DGSI. *Au départ, les demandes sont assez simples à satisfaire, avec quelques recherches sur Internet. Par la suite, elles se font plus précises, et portent sur des sujets plus sensibles, pour lesquels vous devez mobiliser votre réseau ou vos accès à des informations restreintes.* » Cette technique a aussi été employée avec des étudiants à la recherche d'un stage. Les « tuteurs responsables » réclamant aux candidats, par exemple, qu'ils leur fournissent, lors d'une rencontre, des rapports réalisés à l'occasion de stages dans d'autres entreprises… ■

LES 8 COMMANDEMENTS

1 **Ne croyez pas à une offre qui semble trop belle** pour être vraie, car il s'agit probablement d'un piège.

2 **Ne fournissez jamais d'informations personnelles** sensibles et ne faites aucun paiement à des personnes ou à des entreprises que vous ne connaissez pas.

3 **Effectuez des recherches** et vérifiez à qui vous avez affaire avant de donner suite à une proposition.

4 **Maintenez à jour vos logiciels de sécurité** sur votre ordinateur.

5 **Abstenez-vous toujours de cliquer** sur des liens douteux.

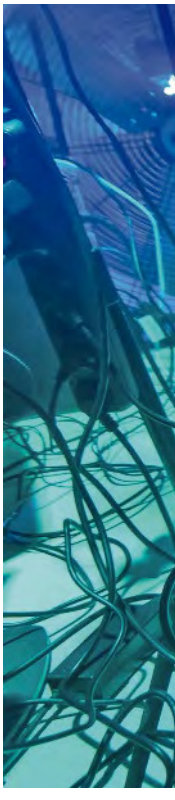
6 **Contrôlez l'adresse de l'expéditeur :** un e-mail frauduleux utilise souvent une adresse ressemblante, mais légèrement modifiée.

7 **Ne cédez pas au sentiment d'urgence.** Les arnaqueurs vous poussent à agir vite (« offre limitée », « compte bloqué »…). Prenez toujours le temps de vérifier.

8 **Activez l'authentification à deux facteurs (2FA).** Cela ajoute une protection à vos comptes, même si votre mot de passe est compromis.

Darknet UN FLORISSANT MARCHÉ NOIR

Les offres de données personnelles volées ne cessent de croître sur le Darknet, si bien qu'il n'y a qu'à tendre la main pour en ramasser. Focus sur une activité en pleine expansion.



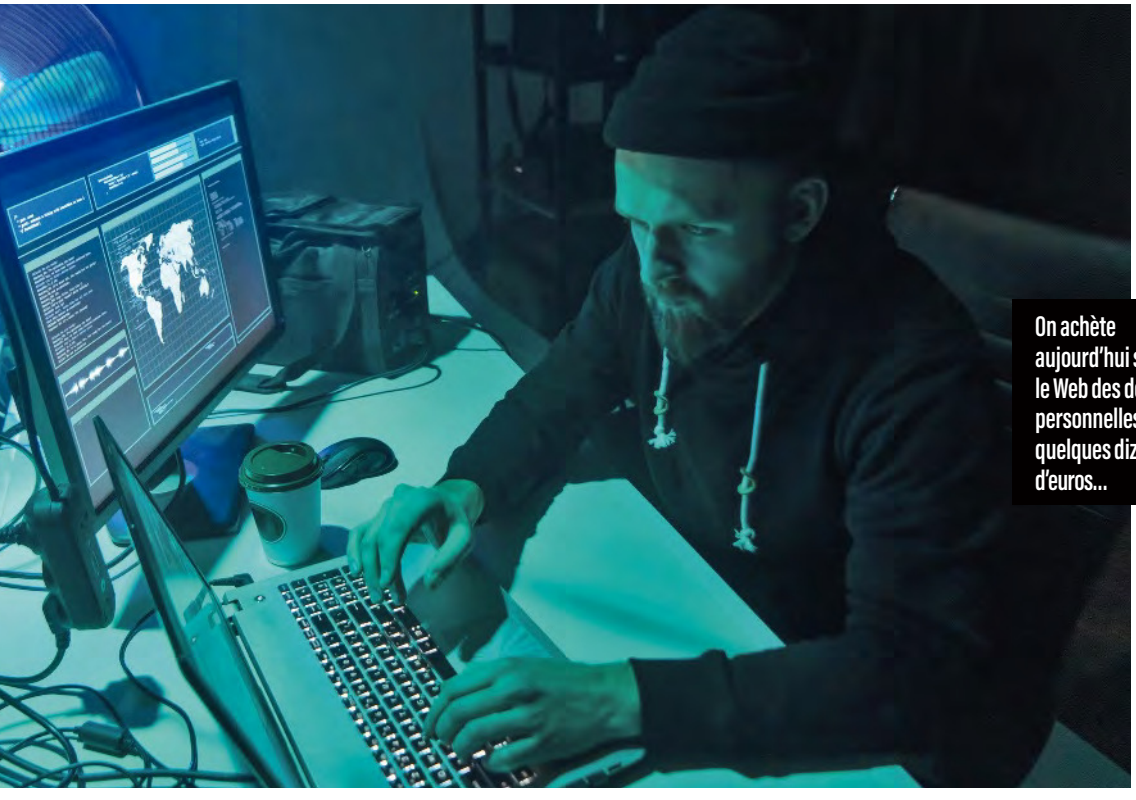
Prénommé Karys (un pseudonyme), il fait partie de cette nouvelle génération d'escrocs informatiques spécialisés dans le commerce de données piratées. Il habite en Europe, mais ne veut pas dire où – en réalité, il pourrait aussi bien être Belge ou Français que Canadien ou Chilien. Il vit, depuis sept ans, de la vente de bases de datas volées à des sites web, ou de la constitution de «combos», autrement dit des regroupements de dizaines de milliers d'adresses électroniques et mots de passe provenant de centaines de sources différentes. *«Tout a commencé quand j'ai eu besoin d'un identifiant de connexion permettant de regarder des matchs de football en streaming,* explique-t-il. *À l'époque, j'avais pu en acheter une dizaine pour 5 €. J'ai très vite compris que le potentiel financier était énorme.»* Le juteux business de la malveillance est alors devenu le sien.

Les acheteurs sont au rendez-vous

Aujourd'hui, Karys dispose de plusieurs boutiques sur le Darknet et sur le Web classique. Il commercialise des accès à Canal+, Disney+ et Netflix, mais aussi à des comptes e-mails, des cartes de fidélité, etc. *«Avec les centaines de milliers d'applications commerciales qui existent, il y a toujours une donnée à vendre, et il y aura toujours des acheteurs. Des gens qui ne veulent pas payer le prix fort pour regarder leur série préférée, par exemple.»* Sans scrupules, Karys ? En fait, il ne se sent simplement pas concerné ! Comme le ferait un personnage du film *Le Parrain*, il affirme que son trafic 2.0 n'a rien de personnel, que *«c'est juste du business»*. Peu prolixe sur les sources des contenus qu'il écoule, il dit les récupérer auprès d'autres pirates, des petites mains qui infiltrent des sites, pratiquent le phishing (hameçonnage) et lui revendent le fruit de leurs larcins. Les prix varient selon les pays, le nombre d'informations, la renommée du site. *«Il n'est pas rare de payer quelques centaines d'euros pour une base de données de milliers de personnes. Il suffit qu'elles contiennent des adresses électroniques, des mots de passe, des numéros de téléphone. J'aurai toujours des acheteurs rien que pour ces trois données»,* assure le malfrat. L'homme indique être en lien avec des Brésiliens, des Thaïlandais et des Indiens. *«J'ai de bons clients en Inde. Ils ont un site qui permet d'acquérir n'importe quel accès à quasiment n'importe quelle chaîne de télé à péage [payante] dans le monde.»* Karys estime que son «travail», comme il l'appelle, continuera tant que les internautes se serviront de la même adresse électronique et du même mot de passe sur chaque site fréquenté. *«Il m'est arrivé d'avoir des dizaines d'accès différents pour le même internaute,* se félicite le pirate. *Il exploitait le même identifiant de connexion sur toutes les boutiques en ligne et les forums auxquels il était abonné.»* En d'autres termes, pour éviter de voir ses accès volés, mieux vaut ne pas suivre l'exemple de cet imprudent. D'autant que cela semble être l'une des meilleures armes pour combattre les pirates.

Récolte de données à grande échelle

Certains malfaiteurs vont encore plus loin dans l'arnaque, se moquant éperdument des conséquences de leurs agissements pour les particuliers et les sociétés dont les datas ont été exfiltrées. Leur



On achète aujourd'hui sur le Web des données personnelles pour quelques dizaines d'euros…

ACRONYM/ADOBE STOCK

credo ? Tant pis pour eux ! Ils considèrent que tout se vend et tout s'achète. C'est ainsi qu'en quelques clics, un particulier a la possibilité de savoir chez quel opérateur téléphonique vous êtes abonné, de retrouver votre adresse et même vos coordonnées bancaires. Science-fiction ? Pas du tout.

Encore discret, un service se développe dans les milieux cybercriminels: le *provider lookup*. Son principe est simple: des plateformes clandestines, accessibles sur le Darknet ou sur des messageries chiffrées comme Telegram, proposent, moyennant quelques dizaines d'euros en cryptomonnaie, d'interroger une gigantesque base de données pour trouver des informations précises liées à un nom, un numéro de téléphone ou une adresse e-mail. Or, ces éléments sont issus de fuites et d'attaques massives… En France, des enquêtes ont révélé que des opérateurs de téléphonie mobile comme Bouygues Telecom, Free et SFR, ou encore leurs filiales low cost, avaient été visés. Les données disponibles incluent des numéros de contrats, des adresses, des identités complètes, voire les RIB associés aux abonnements. De quoi nourrir d'innombrables escroqueries, de l'arnaque au faux conseiller bancaire au détournement de lignes téléphoniques en passant par des usurpations d'identité.

Être un cybercriminel devient beaucoup plus facile

Cette pratique illustre à la fois la démocratisation et la professionnalisation du cybercrime. Autrefois réservées à quelques pirates expérimentés, ces données sensibles sont désormais à la portée de n'importe quel escroc doté d'un portefeuille en cryptomonnaie. L'offre est automatisée; certains services *lookup* revendiquent l'accès à des milliards d'informations mises à jour régulièrement… Résultat: des campagnes d'arnaques personnalisées sont montées en quelques heures, ciblant les victimes avec une précision chirurgicale. De fait, un malfrat qui sait à quel opérateur vous êtes rattaché et dispose de suffisamment d'éléments (nom, adresse, références de contrats) pour crédibiliser son discours peut se faire passer pour lui… L'escroquerie au téléphone ou par courriel s'avère alors bien plus difficile à déjouer. ■

Victimes QUELLES DÉMARCHES SUIVRE ?

Se faire arnaquer sur Internet est un risque qu'il faut prendre en compte. Vous étiez pourtant prudent, mais un pirate a su vous embobiner. N'hésitez pas à signaler les faits et à porter plainte.

Escroqueries à l'amour, arnaques à la cryptomonnaie ou aux faux placements en Bourse, mais aussi virements frauduleux, petites annonces piégées, tentatives de phishing… les menaces sur la Toile pullulent. Cependant, pas beaucoup plus que dans notre vie quotidienne, en réalité ! La différence, c'est qu'en ligne, les assauts sont plus concentrés et plus rapides, à cause des multiples connexions qui émaillent nos existences à l'heure du tout-numérique.

PEINES ENCOURUES PAR LES ESCROCS

L'article 313-1 du Code pénal donne la définition d'une escroquerie: elle consiste à obtenir un bien, un service ou de l'argent par la tromperie. On vous réclame une somme pour un achat ou un voyage fictifs ? On vous fait miroiter un retour sur investissement multiplié par cinq ? Pensant votre interlocuteur honnête, vous l'avez payé de votre plein gré. Or, l'oiseau s'est envolé après vous avoir plumé. Sachez qu'il risque cinq ans de prison et 375 000 € d'amende si on l'attrape.

Lorsqu'une arnaque a pour but la collecte de données à caractère personnel (en utilisant la technique du phishing, par exemple), la loi considère cette action comme frauduleuse, déloyale ou illicite (art. 226-18 du code précité), et celui qui en est à l'origine risque jusqu'à cinq ans de prison et 300 000 € d'amende. En revanche, dans le cas des usurpations d'identité, qui sont pourtant légion, les malfrats encourent une peine moins lourde: un an d'emprisonnement et 15 000 € d'amende (art. 226-4-1 du code précité).

IL FAUT PORTER PLAINTE

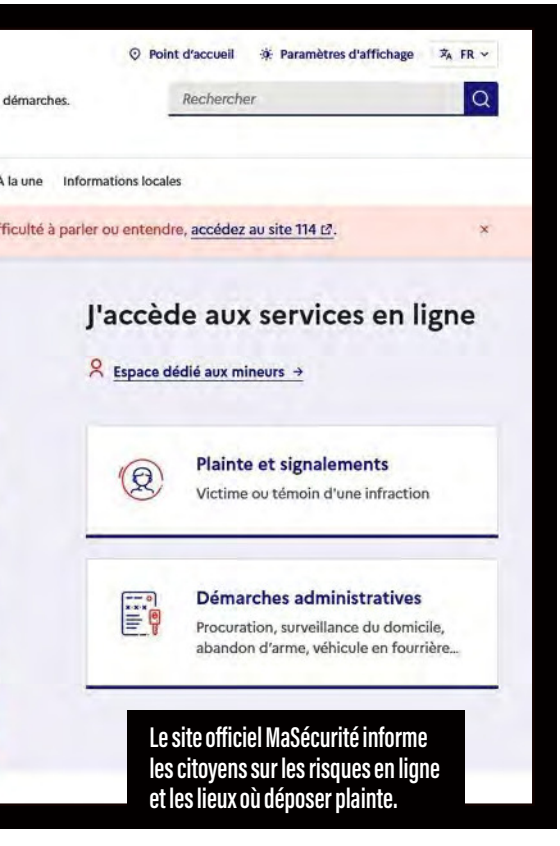
Ne pensez pas que les escrocs demeurent intouchables; ils ne le sont que si aucune plainte n'est déposée… Car les forces de l'ordre ne lâchent rien et parviennent parfois à les coincer. Ainsi, en 2025, à l'issue de plusieurs mois d'enquête, des forums cybercriminels tels que BreachForums ou XSS, d'importants repères de pirates, ont été fermés par les autorités. Pour le premier,

au moins quatre Français ont été arrêtés. Pour le second, un administrateur a été interpellé à Kiev par la police ukrainienne à la demande de la justice française.

Depuis octobre 2024, il est possible de porter plainte en ligne via le site MaSécurité (lire ci-dessous). Finie la pré-plainte nécessitant un déplacement: pour certains vols, dégradations ou escroqueries avec auteur inconnu (hors Internet), la démarche est 100% dématérialisée. Un gain de temps majeur, même si certains cas exigent un rendez-vous au commissariat ou à la gendarmerie. Les plaintes pour infractions cyber (hameçonnage, usurpation d'identité en ligne, piratage, cyberharcèlement…) peuvent, elles, être déposées via la plateforme publique 17Cyber (lire plus bas).

LES ADRESSES UTILES

C'est à juste titre que les autorités encouragent les personnes victimes à dénoncer les faits délictueux en ligne. Il existe plusieurs sites dédiés aux plaintes à la suite d'actes malveillants commis sur Internet. Même si la plupart de ces services publics (gratuits) ne proposent que de faire des signalements, ils s'avèrent utiles.



Le site officiel MaSécurité informe les citoyens sur les risques en ligne et les lieux où déposer plainte.

CAPTURE D'ÉCRAN MINISTÈRE DE L'INTÉRIEUR

> **Perceval** s'adresse aux personnes ayant subi une ou des fraudes à la carte bancaire. Accessible via FranceConnect [1], cette plateforme permet de signaler des cas de phishing, d'escroquerie aux faux placements (*trading*), etc. Avant de vous connecter, assurez-vous d'être toujours en possession de votre carte bancaire et d'avoir fait opposition auprès de votre établissement.

> **Pharos** est l'acronyme de Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements. Elle est dédiée à la lutte contre des propos ou des comportements illégaux sur Internet [2]. On peut y dénoncer des faits de pédophilie, de racisme, d'incitation à la haine ou encore d'apologie du terrorisme.

> **Thesee** [3], acronyme de Traitement harmonisé des enquêtes et signalements pour les e-escroqueries, est un dispositif visant à pouvoir déposer une plainte, dans certains cas, ou à signaler une infraction relevant de la cybercriminalité (sites marchands malveillants, faux courriels, relations virtuelles malintentionnées…).

> **MaSécurité** [4] est un site officiel utile aux citoyens pour retrouver toutes les informations relatives à leur sécurité: annuaire des commissariats ou des gendarmeries, fiches pratiques sur les arnaques en ligne, etc. Avec cet outil, la gendarmerie nationale et la police accompagnent également les victimes dans leurs démarches après coup (plaintes, signalements de fraude, etc.). Enfin, il est possible d'y échanger en direct, via un espace de discussion en ligne, avec un gendarme ou un policier.

> **17Cyber** [5] est une plateforme publique française d'assistance en ligne contre la cybermalveillance. Gratuite et disponible 24 heures sur 24, elle permet aux particuliers, entreprises et collectivités de diagnostiquer une attaque, d'obtenir des conseils personnalisés et, si besoin, d'être mis en relation directe avec des policiers ou des gendarmes spécialisés en cybercriminalité. ■

(1) Service-public.fr/particuliers/vosdroits/R46526. (2) Internet-signalement.gouv.fr. (3) Service-public.fr/particuliers/vosdroits/N31138. (4) Masecurite.interieur.gouv.fr. (5) 17cyber.gouv.fr/ou via le site partenaire Zataz.com/17cyber.

ILS RENFORCENT **VOTRE SÉCURITÉ**

Des logiciels vous permettent de disposer d'identifiants de connexion non seulement très robustes, mais aussi chiffrés et stockés à l'abri. Explication.

Vous souhaitez lire votre journal numérique ? Mot de passe ! Faire des achats en ligne ? Mot de passe ! Relever vos e-mails, payer vos impôts, consulter vos remboursements de Sécurité sociale, de mutuelle ? Mots de passe à chaque fois… Chacun d'entre nous doit aujourd'hui jongler avec des dizaines d'identifiants. Au quotidien, cette gestion est devenue une corvée. Des logiciels visent précisément à nous l'épargner… Ces gestionnaires de mots de passe, disponibles sur ordinateur et sur smartphone (Android, iOS), stockent ainsi tous vos codes derrière un unique mot « maître » (à mémoriser impérativement !). Une fois que l'outil est installé, il faut télécharger une extension pour votre navigateur. Vous importerez ensuite vos mots de passe existants, automatiquement ou en les saisissant un par un. Le gestionnaire les gardera en mémoire et vous suggérera de changer les moins sûrs. Et, grâce à un générateur intégré, il vous proposera automatiquement un mot de passe si vous créez un compte sur un site.

Informations chiffrées

Chaque fois que vous démarrez votre ordinateur, vous devez saisir votre mot de passe maître. Vous êtes ainsi assuré, si quelqu'un d'autre utilise l'appareil, qu'il n'aura pas accès à tous vos comptes. Ensuite, lorsque vous ouvrirez votre navigateur internet (Chrome, Firefox, Internet Explorer, etc.) et irez sur Facebook, Gmail, Ameli.fr ou Impots.gouv.fr, les champs « login » et « mot de passe » seront préremplis. Certains logiciels offrent différentes options de partage (connexion d'un tiers) ou un espace en ligne pour stocker les documents personnels et y accéder depuis n'importe quel ordinateur connecté au Web (lire aussi notre test sur la sauvegarde en ligne, p. 39).

Confier la gestion de tous ses mots de passe à un logiciel unique, et donc à l'entreprise privée qui l'a développé, est anxiogène. Que se passera-t-il si elle met la clé sous la porte ? Si elle est victime d'une attaque informatique ou d'une fuite de données ? Évidemment, le risque zéro n'existe pas. Mais les informations sont chiffrées côté utilisateur, et la clé de chiffrement qui permet d'accéder aux données du compte dépend du mot de passe maître. Rien de ce qui est acheminé vers les serveurs du gestionnaire de mots de passe n'est, a priori, exploitable par quiconque. Lors de nos essais, nous n'avons détecté aucun manquement critique côté sécurité. Ajoutez à cela un constat basique : il n'existe, à ce jour, aucune solution plus sûre pour conserver ses mots de passe. ■

Test

12 SOLUTIONS GRATUITES ET PAYANTES ANALYSÉES

★★★ très bon ★★ bon
★ moyen ■ médiocre
■■ mauvais ● oui - non
n.a. : non applicable.

		Performances – Utilisation ordinateur			Performances – Utilisation smartphone											
		ACHAT/INSTALLATION	CONFIGURATION	UTILISATION COURANTE	IOS	ANDROID	SÉCURITÉ	FONCTIONNALITÉS	NOTE SUR 20	APPRÉCIATION	PRIX €/an	Stockage de documents personnels	Compte multi-utilisateur sur le même poste possible	Import automatique des mots de passe enregistrés dans le navigateur	Remplissage automatique des formulaires	Permission de connexion à un tiers sans donner le mot de passe
1	**NORDPASS** PREMIUM	★★★	★★	★★★	★★	★★	★★	★★★	**15,7**	★★	35,88	●	●	●	●	●
2	**ROBOFORM** PREMIUM	★★★	★★	★★	★★	★★	★★	★★	**15,5**	★★	29,88	-	-	●	●	●
3	**LASTPASS** PREMIUM	★★	★★	★★	★★★	★★	★★	★★★	**15,4**	★★	34,80	●	-	●	●	●
4	**DASHLANE** PREMIUM	★★★	★★	★★	★★	★★	★★	★★★	**15,1**	★★	17,80	●	-	●	●	●
5	**STICKY PASSWORD** PREMIUM	★★★	★★	★★★	★	★★	★★	★★	**15**	★★	29,95	-	-	●	●	●
6	**KEEPER** PERSONNEL	★★★	★★★	★★	★★	★★	★★	★★★	**14,9**	★★	39,99	●	-	●	●	-
7	**1PASSWORD** INDIVIDUEL	★★★	★★	★★	★★★	★★	★★	★★★	**14,9**	★★	31,80	●	●	●	●	-
8	**BITWARDEN** PREMIUM	★★	★★	★★	★★	★★	★★	★★★	**14,6**	★★	12	●	●	●	●	-
9	**PROTON PASS** PASS PLUS	★★	★★	★★	★★	★★	★★	★★★	**14,3**	★★	35,88	●	-	●	-	-
10	**ZOHO VAULT** STANDARD	★	★	★★	★	★	★★	★★★	**12,9**	★★	10,80	●	-	●	-	●
11	**KEEPASSXC** PASSWORD MANAGER	★	★★	★	n.a.	n.a.	★★	★★	**12,7**	★★	0	●	●	●	-	-
12	**ENPASS** INDIVIDUAL PLAN	★★	★	★	★★	★	★	★★★	**12,3**	★★	21,49	●	-	●	●	-

NOTRE MÉTHODE

Nous testons la facilité d'emploi en achetant des licences sous Mac et Windows, en les configurant (création du compte, du mot de passe maître, imports des identifiants du navigateur, etc.) puis en utilisant les logiciels au quotidien.
Nous vérifions que les données sont protégées (force, biométrie, etc.) et que les fonctions attendues sont présentes.

USERBA011D64/ISTOCK

Le meilleur

NordPass PREMIUM
35,88 €/an **15,7/20 | ★★**

NordPass Premium est plutôt simple à configurer et à utiliser au quotidien. Les mots de passe sont illimités et leur niveau de sécurité est correct. Le mot de passe maître protège bien tout ce que le logiciel stocke, y compris les documents personnels. Les données sont chiffrées et l'éditeur ne peut pas y accéder. Dommage que l'aide en ligne ne soit proposée qu'en anglais !

L'alternative

Dashlane PREMIUM
17,80 €/an **15,1/20 | ★★**

Aussi riche en fonctions (mots de passe illimités, stockage de fichiers personnels…) et tout aussi performant, Dashlane Premium coûte moins cher et dispose d'une aide en français.
Son ergonomie est satisfaisante et, côté sécurité, vous pourrez partager l'accès complet avec un tiers de confiance. Un « calculateur de force » vous dit si votre mot de passe maître est assez robuste.

INSTALLER ET CONFIGURER **NORDPASS PREMIUM**

NordPass Premium est le meilleur parmi les gestionnaires de mots de passe que nous avons testés. ● **Objectif :** profiter des fonctionnalités de ce logiciel sur un ordinateur et un smartphone. ● **Niveau de difficulté :** assez facile. ● **Temps nécessaire :** 15 à 20 min.

CHOISIR LA BONNE FORMULE

NordPass Premium est un logiciel de gestion de mots de passe dont la licence, pour un seul utilisateur, coûte 36 € par an. L'éditeur propose aussi une offre famille (jusqu'à six utilisateurs, 67 €/an) et un compte gratuit limité à une personne sur une seule machine. Commencez par là avant de sortir la carte bancaire, afin d'être sûr que cet outil vous convient. La version que nous avons testée (36 €/an) intègre un générateur de mots de passe solides, permet d'en sauvegarder autant que souhaité et de les synchroniser sur tous les appareils. Il est possible de stocker des documents, fonction qu'assurent aussi les solutions de sauvegarde en ligne (lire p. 38). Comme les autres gestionnaires de mots de passe, il fonctionne sous Windows et Mac, ainsi que sur les iPhone et les smartphones Android. Une fois l'offre choisie (image 1) et votre e-mail renseigné (image 2), il faudra installer une extension à votre navigateur web, qui servira d'interface au quotidien. Bonne nouvelle, celle-ci est en français (contrairement à celle de votre compte sur le site de NordPass).

IMPORTER DES MOTS DE PASSE EXISTANTS

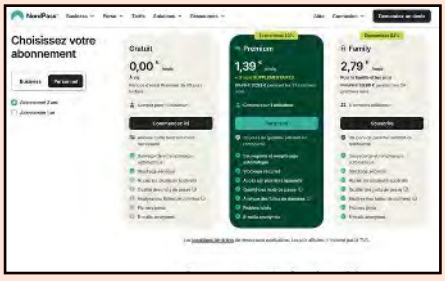
En plus du mot de passe de votre compte, vous devrez définir un mot de passe maître, qui sera utilisé pour déchiffrer votre coffre-fort NordPass (image 3). C'est-à-dire toutes les infos stockées, donc ne l'oubliez pas ! Vous êtes maintenant en mesure d'importer dans le logiciel les identifiants que vous conserviez déjà dans votre navigateur web (et même ceux que vous gardiez dans un autre gestionnaire de mots de passe, comme LastPass ou Dashlane). Rendez-vous dans le menu « Mots de passe du navigateur » et choisissez « Exporter mes mots de passe ». Un fichier en .csv sera généré, qu'il vous faudra alors glisser dans NordPass. Vous retrouverez ensuite vos mots de passe dans l'interface du gestionnaire (image 4).

AU GESTIONNAIRE DE JOUER !

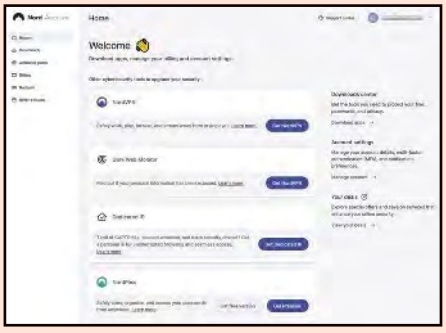
Une fois l'extension installée, NordPass est configuré dans le navigateur comme gestionnaire de mots de passe. Il vous en propose alors automatiquement un lorsque vous êtes invité à créer un compte sur n'importe quel site internet (image 5), grâce à son générateur intégré. NordPass peut gérer plusieurs comptes pour un même site web, en affichant un pop-up qui les liste. Il est également capable de remplir différents champs (nom, prénom, adresse postale ou carte de crédit, par exemple). Dans l'interface du logiciel, il sera aussi possible d'ajouter des mots de passe manuellement.

EFFACER UN COMPTE INUTILISÉ

Ne laissez pas traîner d'identifiants dans un logiciel dont vous ne vous servirez pas. Ainsi, si vous n'êtes pas convaincu par la qualité d'un gestionnaire de mots de passe (que ce soit NordPass ou un autre), supprimez votre compte et effacez toutes les données qu'il contient. Dans les menus proposés (en anglais), cliquez sur « Delete your account » et suivez la procédure (image 6). ■

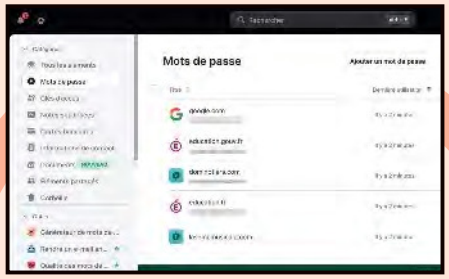


1 Rendez-vous sur Nordpass.com, puis choisissez l'offre qui vous convient entre le compte gratuit, individuel ou famille. Pour la première, pas besoin de sortir la carte bleue ; pour les deux autres, si. Mais vous bénéficierez alors d'une période d'essai de 30 jours.

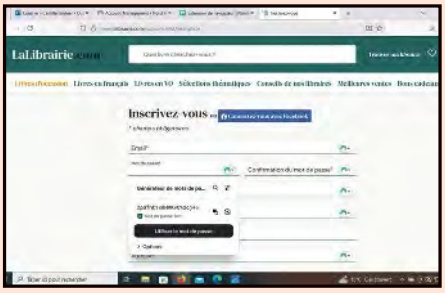


2 Une fois votre adresse e-mail renseignée, NordPass vous propose des services supplémentaires comme NordVPN, une option créant un « réseau virtuel sécurisé », et NordLocker, pour chiffrer vos fichiers. Zappez-les provisoirement. Vous pourrez toujours y revenir plus tard.

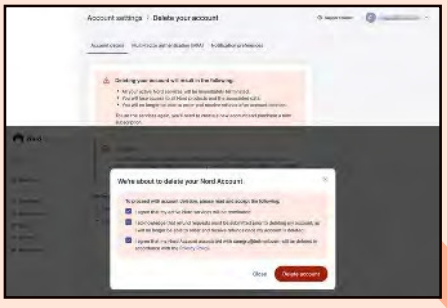
3 La configuration passe par le choix d'un mot de passe maître. Il permet d'accéder à toutes les informations que NordPass stocke. Choisissez-en un solide, en vous reposant sur un moyen mnémotechnique de le retenir. Par exemple, la phrase « Je vais au cinéma le samedi soir » peut devenir « JEvACISS_6-7 ».



4 À cette étape, vous allez pouvoir importer les mots de passe que vous stockiez dans votre navigateur web (Chrome, Firefox, Edge). Exportez-les depuis ce dernier puis glissez-les dans NordPass ; vous les retrouverez ensuite dans l'interface de votre nouveau gestionnaire.



5 Désormais, à chaque fois que vous créerez un compte utilisateur sur un site internet, il suffira de cliquer sur la petite icône verte (symbole de NordPass) pour que les champs requis se remplissent automatiquement et que le générateur intégré suggère un mot de passe robuste.



6 NordPass est le meilleur gestionnaire de mots de passe de notre test. Les autres aussi se montrent performants. Pour autant, si ce type de logiciel ne vous convainc pas, ne laissez pas traîner vos données dedans : supprimez votre compte. La procédure est simple… mais en anglais.

Dons d'animaux
FRAUDES À LA PELLE

Vous avez craqué, via Internet, sur la photo d'un adorable chaton ? Méfiance ! Derrière cette publicité se cache peut-être un malfaiteur.

Les cybercriminels font parfois au plus simple: ils publient des petites annonces sur des sites gratuits. Ils prétendent, par exemple, qu'ils doivent donner leur compagnon à quatre pattes en raison d'un départ en maison de retraite ou d'un déménagement, ou bien que leur chienne a eu des petits dont ils ne peuvent s'occuper. Ils ajoutent des photos de l'animal, bien sûr très mignon, afin de piéger les amis des bêtes plus facilement. Dans 90 % des cas, ils demandent au futur maître de s'acquitter des frais de transport. Parfois, les malfrats proposent des options comme un vaccin, une puce d'identification ou une cage pour le voyage, et prétendent que la somme sera remboursée. Ce n'est évidemment pas vrai !

Méfiez-vous des cartes prépayées

En général, les fraudeurs réclament un transfert par Western Union. Mais, ces derniers temps, l'usage de cartes bancaires prépayées, très simple et ne laissant aucune trace, a leur préférence. « *Pour le règlement du transport,* indique un escroc, *vous devez acheter deux coupons physiques d'une valeur de 150 €.* » Il est possible d'acquérir ces derniers de façon tout à fait légale et très courante auprès de sites spécialisés ou d'un buraliste. Vous versez ensuite la somme sur la carte/ticket puis fournissez le code de la transaction à la personne que vous payez. Grâce à ce numéro, l'arnaqueur touche le montant convenu… et disparaît dans la nature. Autre méthode criminelle souvent utilisée: le faux site d'une entreprise spécialisée dans le transport d'animaux. Si vous essayez de la contacter par téléphone, vous tombez en général sur un répondeur annonçant que la ligne est en maintenance. Parfois, cependant, les arnaqueurs n'hésitent pas à répondre à l'appel afin de convaincre leur correspondant. Peu après la confirmation par le « donateur » de l'expédition du chien ou du chat, la personne qui souhaite l'adopter est contactée, soit par un faux vétérinaire, soit par la société de transport bidon. On lui apprend qu'il y a des frais: dans le premier cas, un vaccin obligatoire est à ajouter; dans le second, en raison de la rareté de la race, il faut acheter une cage appropriée. C'est ici que les voyous plument leurs victimes. Des sommes qui peuvent atteindre plusieurs centaines d'euros pour les plus crédules. Pour

À FAIRE EN CAS D'ESCROQUERIE

Vous avez été victime d'un escroc qui vous a fait croire qu'il allait vous donner un adorable animal ? Ne baissez pas les bras ! Déposez plainte auprès de la police, de la gendarmerie ou du procureur. Pour les escroqueries commises sur Internet, il vous est aussi possible d'utiliser Thesee [1], le service public de dépôt de plainte en ligne du ministère de l'Intérieur, lequel propose aussi des fiches pratiques pour identifier les arnaques et bien réagir. S'il est retrouvé, le malfaiteur encourt 375 000 € d'amende et une peine d'emprisonnement pouvant atteindre cinq ans.

(1) Masecurite.interieur.gouv.fr/fr/demarches-en-ligne/thesee-arnaques-internet-plainte-en-ligne.

Les petites annonces frauduleuses jouent sur la corde sensible pour vous appâter.

BALLABEYLA/ADOBE STOCK

éviter d'en arriver là et démasquer l'escroc qui se cache peut-être derrière une petite annonce intéressante, il convient de ne jamais se précipiter.

Prenez votre temps

Prenez le temps de lire attentivement le message et de vérifier les détails. Les photographies proposées, par exemple, ne se trouveraient-elles pas ailleurs sur Internet ? Demandez des clichés supplémentaires, dans d'autres contextes. Effectuez des recherches sur le vendeur. Vérifiez son identité, son adresse, son numéro de téléphone. Méfiez-vous des demandes de règlement par PayPal, par Western Union, par carte prépayée ou carte-cadeau. Surtout, n'envoyez jamais de l'argent avant d'avoir vu l'animal physiquement. Si possible, rencontrez le vendeur et votre futur compagnon à quatre pattes avant de finaliser la transaction. Bref, si l'offre semble trop belle pour être vraie, c'est probablement une arnaque !

Privilégiez certaines voies

Si vous souhaitez avoir un animal de compagnie, il existe d'autres façons de l'acquérir, en général bien plus sûres que les petites annonces du Web. Vous pouvez vous adresser à des éleveurs ou à des vendeurs professionnels. Les premiers sont spécialisés dans l'éducation de certaines races, ils sont en mesure de fournir des animaux en bonne santé et bien socialisés, avec des papiers d'identification aux normes. Les seconds sont, le plus souvent, des animaleries. Une autre solution est d'adopter auprès d'une association ou d'une fondation de protection animale (lire ci-dessus). Cette option a le mérite de sauver un animal de l'euthanasie ou de conditions de vie difficiles. Il est à noter que les bêtes proposées à l'adoption sont identifiées et vaccinées.

La dernière possibilité est d'adopter un animal donné par une personne de votre entourage (amis, famille, collègues…). Rappelons qu'un particulier possédant une femelle reproductrice n'est pas autorisé à vendre ses petits, sous peine d'être considéré comme un éleveur et d'avoir à se soumettre à diverses obligations réglementaires. ■

Bon à savoir

Les refuges de la Société protectrice des animaux (SPA) ou encore de la Ligue protectrice des animaux (LPA) débordent de chats et de chiens qui n'attendent que vous. Plus d'infos sur La-spa.fr ou Lpa-nf.org.

Comptes piratés
COMMENT BIEN RÉAGIR

Voici l'histoire d'Anna, une médecin qui a dû faire face au piratage de ses messageries professionnelle et personnelle.

Anna (nous avons modifié son prénom) a une quarantaine d'années. Médecin généraliste, elle utilise chaque jour le courrier électronique pour échanger avec ses patients, ses confrères et des organismes administratifs. Résultats d'analyses, ordonnances, certificats… ses boîtes e-mails regorgent d'informations sensibles. Comme beaucoup, elle gère aussi ses affaires privées par courriel: échanges familiaux, factures, documents d'identité. En décembre 2024, elle reçoit un message prétendument signé de son fournisseur de messagerie. On lui indique que sa boîte est *«surchargée»* et qu'elle doit confirmer ses identifiants pour éviter sa suspension. *«Je me souviens que j'étais pressée, entre deux consultations,* raconte-t-elle. *J'ai cliqué et renseigné mon mot de passe sans réfléchir.»* Le pirate, qui vient d'obtenir la clé de son univers numérique, en profite pour installer un logiciel espion dans son ordinateur.

Très vite, Anna remarque des anomalies. Certains patients l'appellent, surpris de recevoir des courriels étranges envoyés depuis son adresse électronique. Le cybercriminel, qui a pris le contrôle, a commencé à fouiller. Il met la main sur des documents officiels, mais aussi sur des correspondances privées. *«Je me suis rendu compte que tout y était: mes papiers d'identité scannés, des relevés,*

Quand votre boîte e-mail est infiltrée, c'est toute votre vie qui est exposée…

TIERNEY/ADOBE STOCK

des infos familiales », détaille-t-elle. L'escroc obtient l'accès à certains de ses outils informatiques professionnels. Il exploite l'adresse de la généraliste afin de piéger d'autres victimes. Il se fait passer pour elle dans le but de soutirer encore plus d'informations. Anna dépose plainte et contacte son hébergeur. Trop tard: certains fichiers circulent déjà sur des forums clandestins.

MESURES À PRENDRE

Cette expérience rappelle que la messagerie électronique est une cible privilégiée. Une seule négligence suffit. Les mesures à prendre sont simples, mais vitales: activer la double authentification, séparer ses usages (pro, perso, administratif), vérifier chaque lien avant de cliquer, chiffrer ou protéger tout document médical ou administratif transmis par courriel. Vous devez fournir des pièces administratives ? Faites-le de manière à les protéger, en les rendant inutilisables par la suite, par exemple en biffant certaines informations (numéro de compte, entre autres). Vous pouvez aussi y ajouter des annotations précisant qui va les recevoir, pour quel type de traitement, etc. N'hésitez pas à contacter le destinataire afin de lui rappeler le Règlement général sur la protection des données (RGPD).

S'IDENTIFIER AVEC FRANCECONNECT

Créé par l'État en 2016, FranceConnect est un système d'identification et d'authentification. Il a été mis en place pour faciliter l'accès sécurisé aux services publics en ligne. Il permet aux citoyens d'effectuer des démarches administratives sans avoir besoin de créer ni de gérer plusieurs comptes. Son fonctionnement est assez simple. Vous vous connectez au service souhaité via votre compte personnel auprès de l'un des sept partenaires d'identification proposés, tels que La Poste, l'Assurance maladie (Ameli.fr) ou encore Impots.gouv.fr. Lors de la première utilisation, vous devez renseigner votre adresse électronique et votre numéro de téléphone, et prouver votre identité. Vous aurez ensuite la possibilité de vous connecter à tous les partenaires de FranceConnect avec vos identifiants. Plus besoin d'en inventer plusieurs…

GARE AU STEALER !

Le *stealer* (ou « voleur numérique ») est un logiciel espion qui exfiltre identifiants, portefeuilles numériques, mots de passe et fichiers sensibles depuis un ordinateur infecté. Comment ça s'attrape ? Il suffit d'une pièce jointe piégée, d'un lien d'hameçonnage ou encore d'un logiciel piraté téléchargé sur un site louche. Ce malware est devenu une vraie plaie sur Internet. Il y en a partout ! Comment découvrir si un *stealer* s'est caché dans votre ordinateur ? Lenteur, comptes e-mails ou réseau social compromis sont des signaux d'alerte. Pour vous en protéger, maintenez vos logiciels à jour ; utilisez un antivirus et, priorité des priorités, ne téléchargez pas n'importe quoi sur votre PC ou votre smartphone. En cas d'infiltration, isolez l'appareil, réinitialisez TOUS vos mots de passe depuis un poste propre et signalez l'incident.

L'un des avantages majeurs de ce dispositif est qu'il garantit la sécurité de vos données personnelles. Testé régulièrement, il repose sur une technologie d'authentification forte qui assure vraiment votre identité. De plus, les éléments transmis lors de la connexion sont protégés par des protocoles modernes. L'Agence nationale de la sécurité des systèmes d'information (Anssi) précise d'ailleurs, dans son rapport d'audit, que cette plateforme, fournie par la Direction interministérielle du numérique, est conforme aux exigences de cybersécurité.

L'usage de FranceConnect présente toutefois quelques inconvénients. Tout d'abord, certaines personnes peuvent être réticentes à partager leurs données avec des tiers. En outre, les services publics ne sont pas encore tous accessibles via le dispositif, et ce dernier connaît parfois des problèmes techniques empêchant d'en profiter. Malgré ces désagréments, il reste quand même très utile pour qui souhaite effectuer des démarches administratives sur Internet en toute sécurité. Depuis sa mésaventure, Anna l'utilise ! ■

Faux policiers
L'IMPOSTURE EN UNIFORME

Vous avez été piégé sur Internet. Vous avez perdu quelques centaines d'euros ou davantage. Vous en parlez sur les forums, cherchez de l'aide… Soudain, un membre des forces de l'ordre vous répond. Attention, danger !

Jeanine a 67 ans. Elle aime dénicher de beaux objets dans des brocantes, des marchés aux puces ou sur Internet. Sauf qu'en ce mois de mai, un flacon en verre du XVIII[e] siècle va lui attirer bien des ennuis. Tout commence par une banale petite annonce sur Facebook. Jeanine craque pour une bouteille peinte à la main de style Louis XVI, selon la vendeuse. La collectionneuse saute sur l'occasion et prend contact avec cette dernière. *« La dame au bout du fil était avenante, connaissait son sujet,* souligne la sexagénaire. *Elle m'a envoyé plusieurs autres photos. Il y avait le flacon et quatre autres, plus petits. J'ai été convaincue, d'autant que le prix me paraissait raisonnable. »* Jeanine débourse 1 100 € pour les cinq objets. Elle n'en verra jamais la couleur. *« Au bout de 72 heures, je me suis inquiétée: plus de nouvelles. La vendeuse ne répondait plus au téléphone et l'adresse électronique ne fonctionnait plus. »* Jeanine comprend qu'elle a été victime d'une escroquerie. *« Je suis allée déposer plainte auprès de la police. Je ne pouvais pas faire opposition, j'ai envoyé l'argent par un mode de paiement proposé par ma voleuse. J'ai laissé des messages sur des forums spécialisés, espérant trouver du soutien, de l'aide pour remonter jusqu'à l'escroc, mais je me suis retrouvée face à des personnes aussi désemparées que moi. »*

Un agent vous écrit

L'histoire aurait pu s'arrêter là. Sauf que 10 jours après cette arnaque, Jeanine est contactée par courriel par un pseudo-policier. *« Il se faisait appeler Jean-Pierre Brau. Il m'a indiqué qu'il travaillait pour une unité de la police et qu'il souhaitait m'aider dans mes démarches. »* L'unité en question, spécialisée dans la lutte contre la cybercriminalité, est baptisée OirccUnit par le pirate. Jeanine lui répond. *« Je lui ai fourni les informations sur ma voleuse, le moyen de paiement, la somme versée, etc. Il m'a déclaré qu'il allait me recontacter rapidement pour la suite de mon affaire. »* Le faux policier rappelle effectivement très vite Jeanine.

À peine 48 heures après leur premier contact, «l'officier» annonce une bonne nouvelle à notre collectionneuse: l'OirccUnit a retrouvé la coupable ! L'argent est *« pour le moment »* sur un compte bancaire domicilié en Suisse. Pour le récupérer, la victime doit régler des frais représentant 20 % du montant volé… Eh bien, savez-vous ce qu'a fait Jeanine ? *« J'ai réglé la somme demandée, sans même me poser de question. J'avoue me sentir un peu honteuse ! J'ai été roulée une seconde fois. J'ai pu me dire que c'était onéreux, mais j'étais*

L'AMF NE RESTITUE PAS L'ARGENT VOLÉ

L'Autorité des marchés financiers (AMF) a lancé, en janvier 2023, une mise en garde contre des escrocs qui prétendent travailler pour elle. Ils se font passer pour ses enquêteurs ou ses agents du service des fraudes et proposent aux victimes d'arnaques aux placements (allant du *trading* de monnaie à la cryptomonnaie) de récupérer leurs fonds. Sachez que, tout comme la police, l'AMF n'est pas habilitée à restituer des sommes perdues par des épargnants.

De faux policiers écument les forums où les victimes s'épanchent… et les piègent une deuxième fois !

ADOBE STOCK

si heureuse de recouvrer mes fonds !» Bilan, Jeanine a perdu 1 320 € au total. Le plus terrible, dans cette histoire, c'est que l'escroc au féminin et le faux policier ne se connaissent pas du tout… Le second voyou écume les forums et les sites traitant d'arnaques, repère les usagers piégés et les contacte. Ceux qui mordent à l'hameçon se font encore avoir ! Bref, qu'il se nomme Jean-Pierre, Francis ou Alphonse, si un inconnu vous téléphone et se présente comme un policier capable de retrouver votre argent et de vous le restituer, raccrochez sans hésiter.

Méfiance sur les espaces de discussion publics

Les malfrats sont également très présents sur les blogs et les forums. Leur méthode est simple: ils diffusent de faux témoignages. Par exemple: *«J'ai été victime d'une arnaque et j'ai perdu une somme importante. Une amie, qui a aussi subi ce genre d'escroquerie, m'a donné l'adresse d'un officier de police d'un organisme de lutte contre la cybercriminalité. J'ai contacté le fonctionnaire et suivi ses instructions. Les escrocs ont été arrêtés et tous les fonds que j'avais perdus m'ont été remboursés. À ceux qui ont connu le même type de mésaventure, je recommande de contacter cet agent.»* Les faux témoignages de ce genre se terminent tous par une adresse électronique spécifique pour joindre le fameux «policier»… Si vous êtes gestionnaire d'un blog ou d'un forum, surtout ne diffusez pas ce type de message. Et alertez les autorités avant de l'effacer. D'ailleurs, afin d'éviter de vous rendre involontairement complice d'une arnaque, vérifiez toujours les posts des utilisateurs avant de les publier. ■

LISEZ BIEN L'URL…

Voici quelques adresses web malveillantes repérées lors de l'écriture de ce hors-série. Il s'agit d'URL usurpant celles de services publics comme la police, la répression des fraudes, l'Assurance maladie ou encore France Travail… Nous sommes notamment tombés sur Services-paiements-amendes.fr ; Amendes-gouvernement.fr ; Ameli-assurecompte.fr ; Dg-ccrf-annule.fr ; Pole-emploie.fr. Soyez vigilant !

Arnaque au RIB
UNE MENACE EN PLEIN ESSOR

Parmi les escroqueries du moment, celle impliquant le RIB cible les services RH. Derrière cette simple demande de changement de coordonnées bancaires se cache une fraude sophistiquée aux conséquences financières lourdes.

Des escroqueries visent les services des ressources humaines (RH) qui gèrent la paye au sein des entreprises: une personne se fait passer pour un employé ou un responsable et envoie une demande de modification de coordonnées bancaires. Une fois le RIB changé, le salaire est versé sur le compte du cybercriminel.

Mesures de sécurité

Ces attaques, qui relèvent de l'ingénierie sociale, s'appuient sur plusieurs techniques: usurpation d'adresses électroniques ressemblant à celles des collaborateurs, falsification de documents, exploitation d'informations internes récupérées via un hameçonnage ou des fuites de données. Le tout est présenté de manière crédible et urgente, incitant les équipes à exécuter la demande sans vérification.

Pour freiner ces fraudes – dont les détournements de virement (52%) et les faux virements par manipulation (39%) – responsables de 351 millions d'euros de pertes en 2024 (+ 12% par rapport à 2023), les banques doivent, depuis le 9 octobre 2025, vérifier la correspondance entre l'Iban et le nom du titulaire avant tout virement. Et alerter leur client en cas d'anomalie… De fait, si vous validez le virement, votre responsabilité est engagée. D'un autre côté, il est recommandé d'instaurer une double validation (oral/écrit), de demander une confirmation systématique via un autre canal (appel téléphonique, rencontre physique) et de sensibiliser les équipes RH. La menace sur les RIB, en pleine croissance, illustre la capacité des cybercriminels à détourner des processus administratifs courants afin d'en faire une source de profits. ■

RESPONSABLE RH CONTOURNEZ LES PIÈGES

> **Vérifiez l'adresse e-mail :** les fraudeurs en utilisent souvent une très ressemblante (ex. : prenom.nom@entreprlse.com au lieu de entreprise.com).

> **Méfiez-vous de l'urgence :** un ton pressant ou une demande de traitement immédiat est un signal d'alerte.

> **Contrôlez les coordonnées :** comparez le nouveau RIB avec les précédents, vérifiez la cohérence du pays ou de la banque. Obtenez confirmation : téléphonez à l'employé ou allez le voir avant d'appliquer la modification.

> **Soyez attentif à la forme du message :** fautes d'orthographe, formulations inhabituelles ou style de langage différent de l'employé ou de la DRH.

> **Mettez en place une double validation :** toute demande de changement bancaire doit être validée par au moins deux personnes, oralement et par écrit.

> **Surveillez les documents joints :** les escrocs envoient fréquemment de faux justificatifs bien imités (carte d'identité, RIB, contrat).

> **Utilisez des alertes internes :** paramétrez vos systèmes comptables ou RH pour notifier automatiquement tout changement de données sensibles.

> **Rappelez ces conseils** sur les fiches de paie.

LE CHANTAGE, TOUJOURS PRÉSENT

Un courriel vous annonce le piratage de votre ordinateur ou de votre webcam. L'escroc dit détenir des informations compromettantes et vous réclame de l'argent contre son silence.

THXSTOCK/ISTOCK

Avril 2018. Des centaines de milliers de courriels menaçants arrivent dans les messageries d'internautes. Ils sont signés d'un individu affirmant avoir infiltré leur ordinateur et y avoir caché un logiciel espion, ce qui lui aurait permis de capter des visites sur des sites pornographiques et, plus grave encore, sur des plateformes pédopornographiques. Cependant, le pirate les «rassure» en affirmant oublier ces images contre quelques centaines d'euros… Ça semble gros, mais des milliers de personnes ont payé. En réalité, le hackeur n'avait jamais eu accès à leurs machines, il n'a fait que joué sur la peur du «qu'en-dira-t-on».

Images trompeuses

Depuis six ans, des arnaques de ce type réapparaissent régulièrement. Les malfrats utilisent les adresses électroniques qu'ils ont récupérées sur des sites, des forums, etc. Il y a quelques années, un escroc franco-ukrainien a été arrêté par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Il se faisait payer 500 € par menace envoyée…

On peut être piégé via une caméra connectée. Les rendez-vous amoureux devant une webcam, par exemple, sont susceptibles de finir avec un chantage orchestré par un individu ayant enregistré ce que vous lui avez montré. Autre possibilité: vous pensiez avoir des tête-à-tête avec votre dulcinée 2.0, mais il s'agit d'une personne qui vous manipule. Une fois un certain niveau de confiance établi entre vous, elle vous demande des renseignements confidentiels, des documents privés (photos, vidéos, etc.). Et cela se conclut par des menaces de diffusion des informations compromettantes obtenues. L'escroquerie à la webcam se produit parfois également sans que la victime en soit même consciente. Des logiciels en apparence légitimes, mais contenant une fonctionnalité malveillante (chevaux de Troie) permettent aux cybercriminels d'accéder à votre caméra (mais aussi à votre micro, aux lettres tapées sur votre clavier, etc.). Il suffit que vous ayez téléchargé un outil piraté sur un site non officiel pour que votre ordinateur soit infecté.

Maximum de prudence

Il existe plusieurs mesures pour vous protéger. D'abord, restez vigilant quand vous communiquez en ligne avec des inconnus. Installez sur votre ordinateur une solution de cybersécurité qui contrera un cheval de Troie. Vous pouvez aussi bloquer l'objectif de votre caméra, cela empêchera toute captation non autorisée (mais le son demeure audible). Enfin, il est fortement conseillé de ne jamais partager d'informations confidentielles en ligne, filmées ou non. ■

UN FAUX PROBLÈME TECHNIQUE

Vous surfez sur le Web, quand une fenêtre s'ouvre et annonce que votre ordinateur a un virus. Le téléphone d'un « service technique » s'affiche…

Une fenêtre d'alerte tonitruante, ça perturbe, c'est sûr ! Mais aucune société sérieuse n'agit comme ça…

Une telle arnaque est courante: alors que vous surfez sur Internet, des pop-up d'alertes surgissent tout à coup sur votre écran; un antivirus semble analyser votre ordinateur. Dans certains cas, un message sonore vous hurle qu'il y a un problème. Votre machine aurait été infectée ! Heureusement, l'une des fenêtres ouvertes vous propose de téléphoner à un service technique…

Appeler, c'est risqué !

Vous composez le numéro. Votre interlocuteur, la plupart du temps une femme, vous demande de décrire l'incident en lui lisant le message apparu sur votre écran. Elle vous confirme un gros souci pour vos données personnelles et vous propose une mise en relation avec un ingénieur. Affable et rassurant, ce dernier a la solution. Il vous demande de le laisser se connecter à votre ordinateur à distance; il utilise pour cela un outil connu, en accès libre. Vous êtes confiant, vous voyez la souris bouger sur votre écran. Le faux technicien vous explique ses manipulations. Il atteste la présence de codes malveillants en vous noyant sous les mots techniques. Vous ne comprenez rien, mais cela semble grave…

Votre ordinateur visité

L'ingénieur vous conseille alors un nettoyage de votre machine et l'installation d'un antivirus meilleur que celui que vous possédez. Il vous vend son service, et vous acceptez de payer ! C'est ainsi qu'en quelques minutes, en plus d'avoir obtenu vos données bancaires, il a eu le temps de fouiller votre ordinateur – la souris que vous regardiez lors de son « audit » était en réalité une vidéo masquant son action malveillante. Il a pu copier vos informations sensibles, installer un outil d'espionnage, effectuer des transactions frauduleuses. Bref, il est trop tard. Sachez-le: aucune société informatique ne vous téléphonera ainsi pour résoudre un problème sur votre PC ! Si vous recevez un appel ou un message de ce type, n'y donnez pas suite, tout est bidon. ■

SI UNE ALERTE APPARAÎT

> **Ne paniquez pas.**
> **Ne composez pas le numéro** de téléphone proposé.
> **Fermez votre navigateur.** Sur PC, appuyez sur les touches Ctrl, Maj et Q simultanément. Sur Mac, appuyez en même temps sur Command et Q.
> **Vous avez appelé et laissé votre ordinateur entre les mains d'un « ingénieur » ? Déconnectez-vous d'Internet.** Analysez votre PC avec un antivirus mis à jour. Dans le doute, récupérez tous vos fichiers essentiels et réinstallez votre machine.
> **Changez l'ensemble de vos mots** de passe.
> **Déposez une plainte** auprès des autorités.

PEOPLEIMAGES/ADOBE STOCK

Trading MIRAGE DE GAINS FACILES

Le *trading* consiste à acheter et à vendre des actifs financiers (actions, obligations, devises…) afin de faire des bénéfices en profitant des variations de leur prix. Cela demande des compétences et ne va pas sans risques de pertes, contrairement à ce que des escrocs tentent de vous faire croire.

Surfant sur l'attrait des cryptomonnaies et des investissements rapides, les escroqueries au *trading* explosent en ligne. Les fraudeurs se présentent comme des plateformes sérieuses ou usurpent l'identité de sociétés régulées, voire de célébrités et d'influenceurs. Objectif: pousser les internautes à investir en leur promettant des rendements spectaculaires.

D'abord on gagne…

La mécanique est bien rodée: après un premier gain fictif destiné à les encourager, les victimes sont incitées à investir de plus grosses sommes pour gagner plus. Mais, lorsqu'elles veulent récupérer leur mise, les retraits deviennent impossibles ou conditionnés à de nouveaux paiements. Certains témoignages font état de pertes colossales, parfois supérieures à 90 000 €.

Techniques de manipulation

L'une des méthodes pour soutirer encore plus d'argent aux victimes est le message qui émane prétendument d'un «département Sécurité & Conformité». Ce courriel vous avertit d'un gel des fonds ou de leur confiscation. Le discours mélange urgence, jargon réglementaire (transactions *on-chain*, score de risque…), menace implicite et preuve vague («Des milliers de personnes ont déjà investi…»). But réel de cette «ingénierie sociale»: vous extorquer des données bancaires et personnelles, des documents d'identité, des frais de déblocage ou de dépôt d'argent. Face à cette manipulation, ne répondez jamais et signalez l'attaque. Vous l'avez compris, mieux vaut prendre des précautions quand on veut placer son épargne. Avant tout investissement, il convient de vérifier que l'intermédiaire figure sur le registre de l'Autorité des marchés financiers (AMF, lire l'encadré ci-dessous). Et méfiez-vous des sollicitations sur les réseaux sociaux. Bref, un principe simple reste d'actualité: si une offre paraît trop belle pour être vraie, c'est probablement une arnaque. ■

5 RÉFLEXES PRÉVENTIFS

> **Vérifiez la régulation** Assurez-vous que la plateforme, ou l'intermédiaire, est bien enregistré(e) sur Amf-france.org, et non sur la liste noire des entités frauduleuses (Amf-france.org/fr/espace-epargnants/proteger-son-epargne/listes-noires-et-mises-en-garde).

> **Méfiez-vous des promesses trop belles** Rendements rapides, « gains garantis » ou absence de risque sont toujours suspects.

> **Contrôlez l'identité du contact** Attention aux usurpations de sociétés connues, d'influenceurs ou de célébrités.

> **Ne cédez pas à l'urgence** Les escrocs mettent la pression (« dernière chance », « offre limitée »). Prenez le temps de vérifier.

> **N'investissez jamais plus que ce que vous pouvez perdre** Commencez par de petites sommes et ne communiquez jamais vos données bancaires sans certitude absolue.

Les bons outils

Bien s'équiper et investir dans la cybersécurité est fondamental. Sans logiciels dédiés à la protection de sa vie privée, les risques sont grands de voir ses données personnelles finir entre les mains de pirates. Dans notre monde connecté, nos machines présentent des vulnérabilités, alors que les menaces en ligne ne cessent de s'étoffer. Si certaines solutions (antivirus, pare-feu…) s'avèrent coûteuses, d'autres sont gratuites. Nous vous présentons ici les meilleures du marché, assorties de conseils avisés pour vous prémunir des dangers au quotidien. Rappelons aussi que si de bons outils sont utiles, les miracles, eux, n'existent pas: la sûreté de notre environnement numérique dépend surtout de nos comportements.

SOMMAIRE

EXENTIA ; PV/ADOBE STOCK

Chiffrement
LA CLÉ DU SECRET

Le chiffrement apparaît comme une solution efficace si vous voulez éviter que des documents numériques soient consultés par des personnes non autorisées.

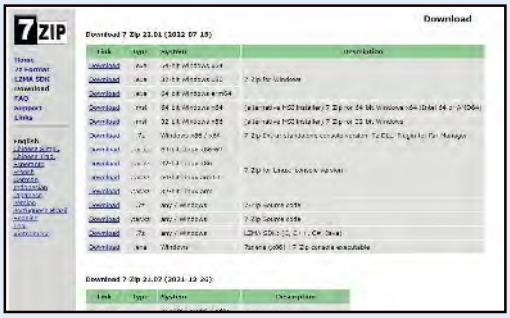
Juin 2021, c'est la stupeur au Royaume-Uni: 50 pages de documents sensibles du ministère de la Défense, dont un classé top secret, sont retrouvés… derrière un arrêt de bus du Kent ! Preuve que la fuite d'informations touche tout le monde, même les mieux formés à la sécurité. Un ordinateur, qu'il s'agisse d'un poste fixe ou d'un portable, sauvegarde un nombre considérable de données. Courriers électroniques, photos, vidéos, mots de passe: il contient parfois toute une vie, personnelle comme professionnelle. Cette existence numérique est consultable par tous ceux ayant accès à cette machine, ce qui peut s'avérer particulièrement préjudiciable s'il s'agit d'individus malintentionnés. Or, les avancées technologiques et la prolifération des réseaux vont de pair avec l'augmentation des menaces de sécurité en ligne – attaques de pirates, logiciels malveillants ou interceptions au vol, comme celle découverte par la police nationale, à Paris, en février 2023. Bref, aujourd'hui, les besoins de protection s'avèrent de plus en plus importants.

Chiffrer ou crypter ?

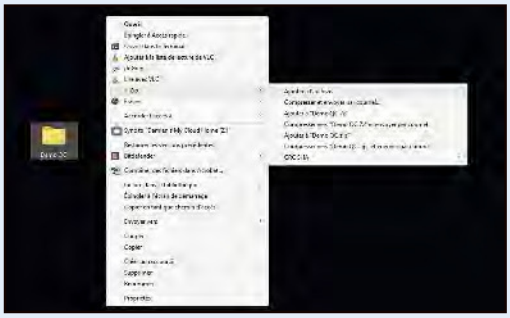
Pour sécuriser leurs données, entreprises, organismes et particuliers peuvent les chiffrer. C'est-à-dire qu'ils les transforment en leur appliquant un code de chiffrement, intelligible uniquement pour la personne ou le système informatique autorisés. Ainsi, même s'il y a une fuite et qu'elles

CRÉER UN CONTENEUR AVEC 7-ZIP

Ce logiciel gratuit sert à regrouper plusieurs fichiers choisis (textes, images, photos) dans un même « conteneur informatique », autrement dit dans un espace où les objets seront stockés sous une forme organisée, selon des règles précises. Son fonctionnement est très simple.



1 Installer 7-Zip sur son ordinateur depuis le site 7-zip.fr.



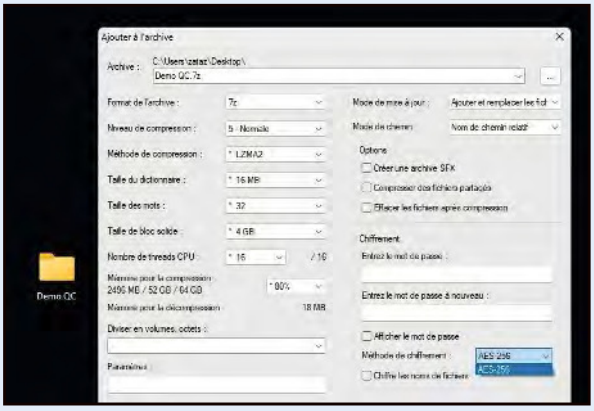
2 Sélectionner le dossier contenant les fichiers que l'on souhaite regrouper dans un même conteneur.

IMAGINIMA/ISTOCK

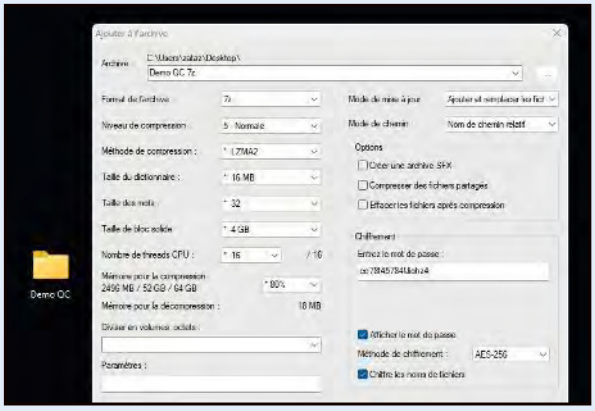
tombent entre de mauvaises mains, les informations conservent leur confidentialité. Plus largement, cette mesure de précaution protège les contenus personnels (codes bancaires, adresse, numéro de téléphone, etc.). En cas de violation de la sécurité, les risques de vol d'identité sont réduits, et les conversations restent secrètes, notamment celles en ligne. En effet, sécuriser des informations circulant sur la Toile commence par le chiffrement des échanges entre les internautes et les sites web. Tout le monde ne le sait pas, mais le dessin du petit cadenas et le «s» à la fin du «https» dans l'adresse d'un site signalent en effet que la communication est chiffrée.

On entend parfois des personnes dire que «le fichier a été crypté». Qu'est-ce que cela signifie? Pas forcément qu'il a été chiffré… Selon son étymologie, la cryptologie est la science des messages secrets. Elle regroupe la cryptographie, qui consiste à écrire de façon cachée (avec du jus de citron sur un papier, par exemple) pour assurer la confidentialité, l'authenticité et l'intégrité de textes; la cryptanalyse, qui cherche à déterminer la méthode employée pour crypter un contenu (et ainsi «casser» le chiffrement); et la stéganographie, qui correspond à l'art de dissimuler un message dans un support (par exemple, dans le code numérique d'une image). La cryptographie emploie souvent des codes secrets ou des clés; le chiffrement en fait partie, car il rend la compréhension d'un document impossible à toute personne n'ayant pas accès à la clé de (dé)chiffrement.

Par ailleurs, rappelons qu'on ne dit pas «encrypter» ni «désencrypter» (il s'agit d'anglicismes), mais bien «déchiffrer» (un texte, par exemple, quand on possède la clé) et «décrypter» (une vidéo, entre autres). Et qu'il est impossible de crypter sans chiffrer avec une clé… Mais alors, qu'en est-il des chaînes de télé «cryptées»? Chiffrer.info explique que, «*dans le cadre de la télévision à péage, on parle quasi exclusivement de chaînes "cryptées", ce que l'Académie française accepte*». Ce site différencie bien les termes coder, >>



3 Cliquer sur le bouton droit et sélectionner « 7-Zip », puis « Ajouter à l'archive ».



4 Entrer le mot de passe qui protégera le conteneur. Choisir « Méthode de chiffrement AES-256 », puis « Chiffrer les noms de fichiers ».

>> chiffrer et crypter. Enfin, si de nombreuses solutions (payantes et gratuites) permettent de se lancer dans le chiffrement, toutes ne sont pas simples à exploiter pour des novices… Nous nous attarderons donc, dans l'encadré ci-dessous, sur les logiciels gratuits et faciles d'accès.

La substitution, mode d'emploi

En guise d'introduction, toutefois, découvrons une méthode de chiffrement vieille comme le monde (et donc non sécurisée), grâce à laquelle on s'initie en douceur: la substitution. Soit le changement de chaque lettre du texte clair par une autre, selon une règle spécifique. Une déclinaison de ce système, appelé le «chiffre de César» (car utilisé par l'homme d'État romain dans ses échanges avec Cicéron), consiste à remplacer chaque lettre par une autre située un peu plus loin dans l'alphabet. Par exemple, avec un décalage de quatre positions, A devient D, B sera E, etc. On obtient alors, pour les mots Que Choisir, la traduction suivante: Txh Fkrlvlu. Le site Dcode.fr/chiffre-cesar propose divers exercices pour s'entraîner au décalage. ■

SÉCURISER UN DOCUMENT GRÂCE À…

▶ BITLOCKER

Outil de chiffrement intégré à Windows, BitLocker sécurise les données du disque dur de l'ordinateur. Pour l'activer, il faut aller dans les paramètres de sécurité de Windows (versions 10 et supérieures) et suivre les instructions. On sélectionne le disque dur à protéger (clic droit de la souris : « Activer BitLocker ») puis on sauvegarde la clé de récupération – ce sésame déverrouille la machine en cas de suspicion d'accès non autorisé aux données. Il est conseillé de la stocker sur un support sûr, non connecté, comme une clé USB rangée dans un tiroir. Une fois BitLocker activé, toutes les données présentes sur le disque dur du PC sont chiffrées automatiquement. Il est aussi possible de protéger de la sorte les supports amovibles (disque dur externe, clé USB, etc.). Les dossiers ainsi sécurisés pourront être lus sur d'autres ordinateurs sous Windows, à condition que l'on dispose du mot de passe de déchiffrement.

▶ VERACRYPT

Ce logiciel open source (son code source peut être étudié et retravaillé) protège dossiers comme disques durs (lire aussi la fiche pratique p. 81). Attention, cependant, à ne pas lancer ce processus sur le disque dur chargé du démarrage et de l'exploitation du PC. Pour protéger un fichier, il suffit de le sélectionner, de choisir l'algorithme de chiffrement (plus ou moins complexe, il le rendra illisible à un tiers) et de créer un mot de passe. Le document codé peut ensuite être stocké sur l'ordinateur ou dans le cloud.

▶ DISK CRYPTOR

C'est l'autre outil grand public de chiffrement. Il sécurise disques durs, clés USB et cartes SD. On sélectionne le disque dur et le dossier visé, puis on choisit la méthode de chiffrement (la DoD 5220.22-M, utilisée par le département de la Défense américain, est conseillée). Enfin, on fournit un mot de passe, et Disk Cryptor évalue sa pertinence ; s'il est trop faible, le logiciel alerte.

▶ SIGNAL

Facile à utiliser, cette application assure la confidentialité des conversations en ligne. Elle emploie un protocole de chiffrement de bout en bout, ce qui signifie que les échanges sont chiffrés sur l'appareil de l'utilisateur et ne peuvent être décodés que par l'interlocuteur. Ce dernier doit lui aussi installer Signal pour sécuriser ses communications. Appli disponible sur Android, iOS et Windows. À noter, elle ne gère plus réception et émission de SMS.

▶ PROTON MAIL

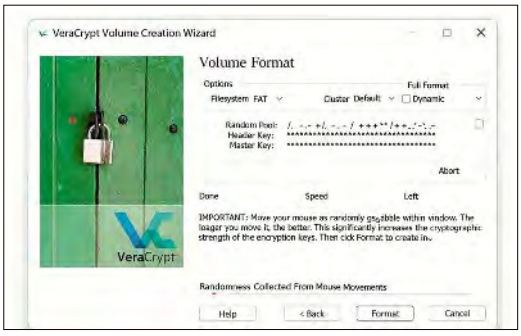
Ce service de messagerie garantit la confidentialité des mails. Les messages envoyés et reçus via ce dispositif sont chiffrés tout du long. Autrement dit, seuls l'expéditeur et le destinataire y ont accès. Simple d'usage et disponible sur Android, iOS et Windows, Proton Mail peut, cependant, ne pas être utilisé par le correspondant ; il faudra alors sécuriser le message par un mot de passe.

Fiche pratique

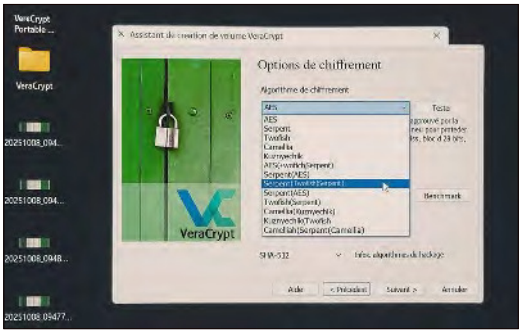
CHIFFRER AVEC VERACRYPT

Voici, en six étapes, comment protéger ses fichiers avec ce logiciel open source.

1 Télécharger le logiciel depuis le site Veracrypt.io et l'installer sur son ordinateur ; l'ouvrir.



2 Sélectionner *Create Volume* (« Créer un volume »), puis *Create an encrypted file container* (« Créer un fichier conteneur chiffré »). Cliquer sur *Next* (« Suivant »), choisir l'endroit où enregistrer le document et le nommer.



3 Choisir l'algorithme de chiffrement (AES est recommandé) et définir un mot de passe fort.

4 Cliquer sur *Next* (« Suivant ») et choisir la taille du volume. Cliquer de nouveau sur *Next* et suivre les instructions pour formater le volume chiffré.

5 Ouvrir VeraCrypt, sélectionner le fichier chiffré et cliquer sur *Mount* (« Monter »). Entrer le mot de passe.

6 Pour retirer le conteneur, retourner sur l'écran principal de VeraCrypt et cliquer sur *Dismount* (« Démonter »). Il ne sera plus accessible jusqu'à la prochaine connexion.

Traces numériques LES GÉRER

Si votre ordinateur est allumé, il laisse des empreintes et cela crée un risque. Elles peuvent être collectées et exploitées de façon malhonnête. C'est pourquoi il est essentiel de savoir les maîtriser et, si besoin, de les effacer.

Les traces numériques les plus courantes laissées par les appareils incluent: journaux d'activité, fichiers temporaires ou de sauvegarde, cookies, historiques de navigation. Autant d'informations sensibles qu'il faut savoir gérer, en particulier avant de revendre une machine.

Un ménage régulier

Un ordinateur privé contient souvent des éléments critiques: données personnelles ou financières, mots de passe, documents professionnels confidentiels… Attention: déplacer des fichiers vers la corbeille, puis la vider, ne suffit pas. Un logiciel de récupération peut les retrouver! Pour qu'une information disparaisse vraiment, elle doit être écrasée par d'autres.

Comment effacer

Les systèmes récents (Windows, MacOS, Linux) ne proposent plus «nativement» (d'origine) de suppression sécurisée simple des données. Voici donc comment procéder pour les effacer totalement sur votre ordinateur:

> **Sur Windows:** la combinaison Maj + Suppr permet une suppression directe, mais non sécurisée. Pour rendre les fichiers irrécupérables, il faut utiliser un outil dédié.

> **Sur MacOS:** Apple a supprimé son option «Vider la corbeille de façon sécurisée». Il est donc, ici aussi, recommandé de se servir d'un logiciel spécialisé pour y parvenir.

> **Solutions dédiées:** BleachBit, CCleaner, DBAN (pour Darik's Boot and Nuke) ou encore Eraser (lire l'encadré p. 84) appliquent des algorithmes d'écrasement répétés, qui rendent les données quasiment impossibles à récupérer. Ces logiciels effaçant les fichiers définitivement, prudence avant de les lancer.

À NOTER Les ordinateurs ne sont pas les seuls concernés. Routeurs, disques durs externes, clés USB ou encore smartphones et consoles de jeux stockent aussi des informations sensibles. ■

CHECK-LIST AVANT DE REVENDRE SON MATÉRIEL

> **Pour les sauvegarder, copier ses fichiers personnels** sur un disque externe ou dans un cloud sécurisé.

> **Se déconnecter de tous ses comptes** (e-mails, réseaux sociaux, services bancaires et logiciels).

> **Supprimer les profils enregistrés dans le navigateur** (Google, Apple ID, Microsoft, etc.).

> **Réinitialiser l'appareil** en utilisant la fonction de restauration d'usine (fournie sur Windows, MacOS, Android, iOS). Cela retire la majorité des données visibles, mais pas toujours définitivement.

> **Effacer de manière sécurisée:** avec un logiciel (BleachBit, DBAN, Eraser…) sur un ordinateur ou en activant le chiffrement avant la réinitialisation sur un smartphone Android (les anciennes données deviennent alors illisibles). Avec un iPhone, il faut aller dans «Réglages > Général > transférer ou réinitialiser », puis sélectionner «Effacer contenu et réglages». On entre son code secret s'il est demandé et on confirme.

> **Vérifier les supports externes:** clés USB, cartes mémoire, disques durs, à effacer ou à garder.

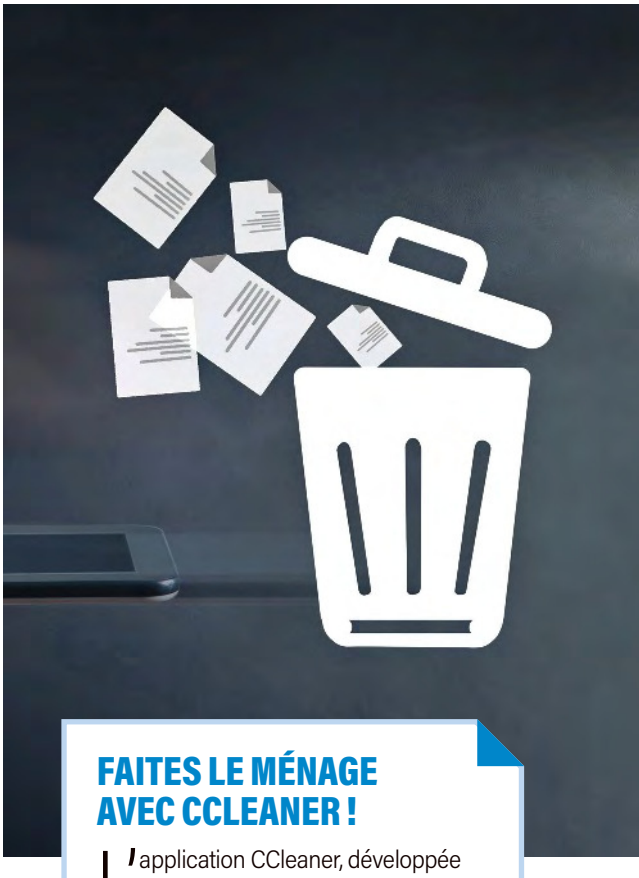
> **Nettoyer les équipements réseau:** réinitialiser routeur/box internet aux paramètres d'usine.

> **Éliminer toutes les configurations** (SSID wifi, mots de passe, identifiants).

> **Contrôler une dernière fois:** en allumant l'appareil après réinitialisation, aucune donnée personnelle ne doit apparaître.

Ordinateur
UN STOCKAGE INFINI

Vous stockez nombre de choses sur votre ordinateur. Et, de son côté, la machine sauvegarde aussi beaucoup d'informations vous concernant…



ARTVIBE/ADOBE STOCK

Une machine est ainsi programmée: elle collecte constamment des données (nom, adresse IP…) qui seront ensuite gardées sur son disque dur et dans sa mémoire vive. Les navigateurs web en récupèrent également (sites visités, formulaires remplis, etc.). L'ordinateur stocke des informations qui concernent aussi bien son propre système (quantité de mémoire vive disponible, processeur utilisé, espace disque libre, mise à jour du système d'exploitation, wifi, Bluetooth…) que les applications qui y sont installées. Il sauvegarde encore les journaux d'erreurs, les rapports de plantage, les mises à jour passées et les historiques de connexion avec des périphériques connectés (clé USB, imprimante, webcam…) pour simplifier leur prochaine utilisation. Enfin, on retrouve dans les mémoires vive ou virtuelle de la machine des traces numériques plus sensibles, comme les mots de passe enregistrés, les informations de carte de crédit ou les conversations en ligne.

À QUOI SERT LA MÉMOIRE VIVE OU PHYSIQUE ?

La mémoire vive, parfois abrégée avec l'acronyme anglais RAM *(random access memory)*, contient toutes les informations produites durant le temps d'utilisation de l'ordinateur, des frappes clavier aux documents ouverts. La mise hors tension permet de les effacer. Cette destruction s'avère plus ou moins longue, c'est pourquoi il est conseillé de rester devant sa machine jusqu'au moment où elle s'éteint. Cela évite notamment un assaut informatique baptisé *cold boot attack* («attaque par démarrage à froid»), >>

FAITES LE MÉNAGE AVEC CCLEANER !

L'application CCleaner, développée par la société anglaise Piriform, permet d'effacer toutes les traces produites par un ordinateur ou par un smartphone lors de son utilisation, avant de l'éteindre. La version gratuite nettoie les navigateurs et les logiciels exploités ; elle détruit les fichiers temporaires, véritables « squatteurs » de disque dur. En contrepartie, il est impossible de retrouver ses dernières actions. Même chose pour les cookies : elle fera le ménage (à télécharger sur Ccleaner.com).

EFFACER LES COOKIES SOUS WINDOWS

Sous Windows, il est possible de supprimer les cookies sans recourir à un logiciel. Pour cela, il faut ouvrir son navigateur web favori et cliquer sur le menu situé dans le coin supérieur droit (représenté par trois points verticaux ou horizontaux). On sélectionne alors « Paramètres », puis on fait défiler la page jusqu'à la section « Confidentialité et sécurité » (ou « Vie privée et sécurité », « Confidentialité », etc.). Il faut alors cliquer sur « Effacer les données de navigation » (ou « Effacer l'historique »). Dans la fenêtre pop-up qui s'affiche, on sélectionne « Cookies et autres données de site » (si on ne veut supprimer que les premiers, on décoche les autres options). La période pour laquelle on souhaite effacer les cookies est aussi programmable : on ira sur « Plage de temps » dans la liste déroulante, avant de cliquer sur « Effacer les données ».

>> soit une tentative de récupération, par des pirates, des informations contenues dans l'appareil au moment de sa fermeture. Pour fonctionner, l'ordinateur lance (écrit) en continu des milliers d'actions, ce qui sollicite énormément sa mémoire vive. Parfois, les limites de celle-ci sont atteintes.

> Les clients d'Apple disposent, en ce cas, d'une « mémoire virtuelle », sécurisée et préconfigurée, dans leur Mac. Ce bloc d'espace peut faire office de mémoire lorsque la RAM n'est plus suffisante pour exécuter activement des programmes; pour cela, il va chiffrer les données écrites de cette dernière sur le disque dur.

> Les possesseurs de PC, quant à eux, peuvent lire sur le Web qu'il est possible d'optimiser la mémoire virtuelle de leur ordinateur en détruisant deux fichiers présents dans le système d'exploitation Windows, intitulés pagefile.sys et swapfile.sys. Il est pourtant fortement déconseillé de le faire, car cela risque de perturber, voire de planter intégralement la machine…

Les traces numériques d'un internaute étant susceptibles d'être employées pour suivre ses activités, on effacera régulièrement, par mesure de protection, les fichiers temporaires (dans Windows, il s'agit du répertoire Temp) et les cookies (lire l'encadré ci-dessus). Les journaux créés par le système d'exploitation de l'ordinateur constituent également des traces écrites des actions menées. Ces historiques détaillés, connus sous le nom de « logs », enregistrent faits et gestes numériques de l'utilisateur (marque et modèle de sa clé USB

DÉTRUIRE DÉFINITIVEMENT SES FICHIERS AVEC ERASER

Eraser est un logiciel de sécurité gratuit pour Windows conçu pour éradiquer les fichiers et les dossiers d'un ordinateur. Après l'avoir installé, on sélectionne le document à détruire (via « Eraser Schedule » ou en le faisant glisser dans la fenêtre d'Eraser). Une option intéressante : la planification de la suppression à une date et une heure précises. Selon la taille du fichier à détruire, cela peut prendre un peu de temps (de l'ordre de plusieurs minutes). Attention, cette action est irréversible une fois lancée. Ce logiciel est à télécharger sur le site officiel, Sourceforge.net/projects/eraser.

M. WILLIAM/ISTOCK

Pour fonctionner au mieux, l'ordinateur enregistre automatiquement nos actions. Mais cela prend de la place !

et de son imprimante, date des impressions, logiciels mis en œuvre, etc.). Or ils sont gardés dans un ordinateur sans limite de temps… Des outils tels que CCleaner (lire l'encadré p. 83) ou Wise Disk Cleaner peuvent les faire disparaître, mais mieux vaut rester prudent, car les logs ont leur utilité. Ils permettent en effet à la machine de ne pas rencontrer une erreur une seconde fois ni de se bloquer.

INTÉRÊT DE LA SURVEILLANCE

Deux solutions gratuites permettent de contrôler l'activité de son ordinateur: ActivTrak et Time Doctor. Elles proposent des fonctionnalités comme la capture d'écran et la surveillance des applications et des sites web visités. Une fois installés, ces logiciels enregistrent ces données et les stockent dans les clouds (espaces de stockage à distance) des deux sociétés qui les éditent. Par conséquent, il faudra se rendre sur Activtrak.com ou sur Timedoctor.com pour les consulter.

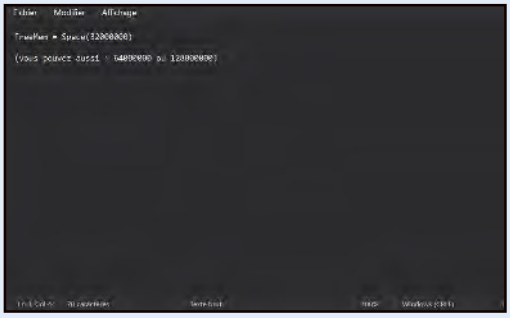
MÉMOIRE DES LOGICIELS

Si un ordinateur sauvegarde énormément d'informations sur les activités de son propriétaire, il n'est pas le seul. Les logiciels de travail – traitement de texte, gestionnaire d'image, navigateur et imprimante, pour ne citer qu'eux – collectent également des tonnes de renseignements. Pour cela, ils créent eux-mêmes des journaux d'actions, autrement dit des informations dans l'information… Les plus connus, et visibles, sont les ensembles de métadonnées générés lors des prises de vues numériques et sauvegardés dans les fichiers images, appelés Exif *(exchangeable image file format)*. On y trouve le nom de l'appareil photo, son numéro de série, l'heure de création de la photographie et sa géolocalisation (si le cliché a été pris avec un smartphone). Le logiciel gratuit ExifTool (sur Exiftool.org) permet de découvrir les secrets des métadonnées de ses documents… et de les effacer au besoin. ■

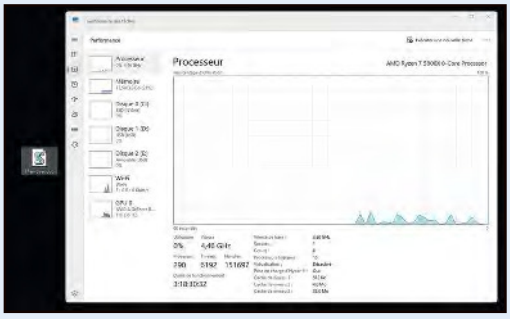
ÉCRASER DES DONNÉES

Avant de fermer votre ordinateur, ouvrez plusieurs images à l'écran. Leur poids écrasera les informations que la mémoire vive a pu collecter. Autre méthode, plus geek : créez un petit fichier sur votre bureau (code ci-dessous) et exécutez-le quand bon vous semble. Des logiciels gratuits comme Wize Memory Opimizer (Wisecleaner.eu/wise-memory-optimizer.html) peuvent vous y aider d'un simple clic.

1 Ouvrez votre outil « Document texte » (Notepad, etc.).



2 Écrivez « FreeMem = Space(32000000) » (il s'agit de la quantité à vider, sachant que 32000000 veut dire 32 Mo de mémoire).



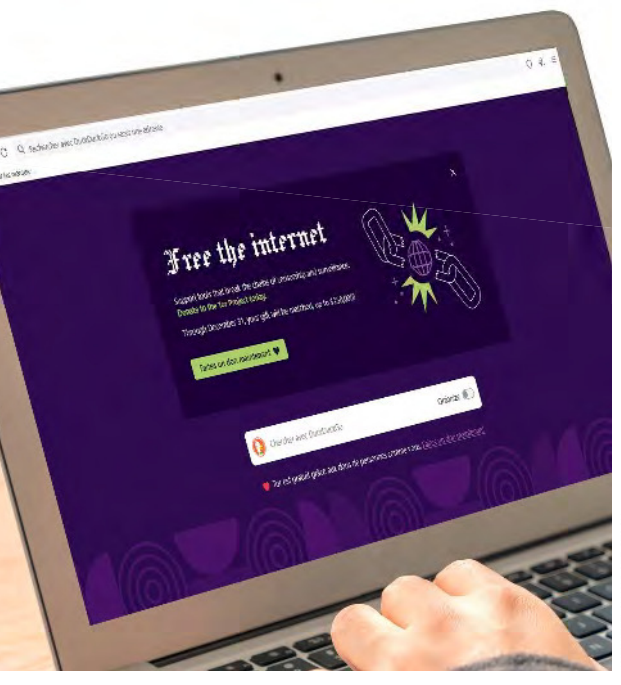
3 Sauvegardez le document avec l'extension .vbs à la place du .txt (Memoire.vbs, par exemple), puis sélectionnez-le pour vider de la mémoire.

TOR LE SURF INCOGNITO

Vous souhaitez naviguer sur Internet sans laisser de traces ni de quoi vous géolocaliser ? C'est possible avec le navigateur TOR.

TOR (acronyme de The Onion Router) n'est pas un réseau comme les autres. Son objectif: vous donner accès à Internet de manière privée, anonyme. Il permet également à un site web qui passe par lui de cacher son identité ainsi que sa géolocalisation. Quand vous le visitez, il ne sait pas qui vous êtes, mais vous ne savez pas qui il est…

L'usage de ce réseau exige de le paramétrer, tout comme les logiciels dont vous vous servez, ce qui peut être fastidieux. Pour vous simplifier les choses, une solution dédiée a été conçue (Torproject.org), qui inclut le logiciel TOR et le navigateur Firefox configuré pour fonctionner avec. Facile à installer et à utiliser, elle ne nécessite pas de paramétrage supplémentaire. Pour acheminer vos connexions sans que vous soyez identifiable, TOR emploie des machines reparties à travers le monde entier. Ces ordinateurs font partie d'un «circuit» qui vous est alloué le temps de votre navigation. Une fois le navigateur fermé, ce circuit est annulé; il sera modifié lors d'une prochaine utilisation.



INFINITEFLOW/ADOBE STOCK

Connexions simples et complexes

Le réseau comporte, par exemple, une machine en Suisse, qui se connecte à une autre en Belgique, qui passe par une troisième aux États-Unis, pour enfin joindre le site voulu. Les URL peuvent avoir deux formes: classiques (Ufc.quechoisir.org, par exemple) ou se terminant par .onion (comme pour le moteur de recherche DuckDuckGo: Duckduckgo.gg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion). Les adresses de ce type ne marchent pas dans un navigateur classique.

Pour que le circuit soit modifié, et changer de pays de connexion, il suffit de cliquer sur le petit logo en forme d'oignon présent dans la barre d'adresse. Enfin, en allant sur le bouclier en haut à droite du navigateur, il est possible de modifier les paramètres de sécurité et d'augmenter le niveau de protection (cookies, etc.). Attention, cela peut empêcher certains sites web de fonctionner correctement.

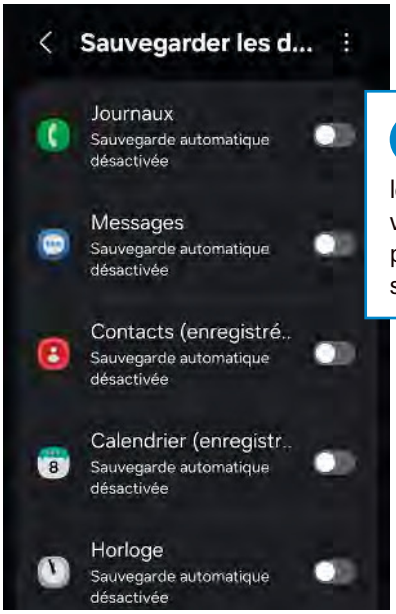
Sécurisé à 100 % ?

Il faut noter que le navigateur TOR, s'il permet de naviguer sur Internet en masquant son adresse IP, ne garantit pas l'anonymat de l'ensemble des connexions internet de l'ordinateur. Concrètement, vos données passent par plusieurs «relais» chiffrés avant d'atteindre leur destination, ce qui complique la surveillance. TOR est donc pratique pour protéger sa vie privée ou accéder à des sites bloqués. Mais attention: cette solution n'est pas sûre à 100 %. Si vous vous connectez avec vos vrais comptes (ex. Gmail, Facebook), ou si la page sur laquelle vous surfez n'est pas en https, votre identité peut être retrouvée. Utiliser TOR doit toujours s'accompagner de bonnes pratiques de sécurité, et parfois d'un VPN en complément. ■

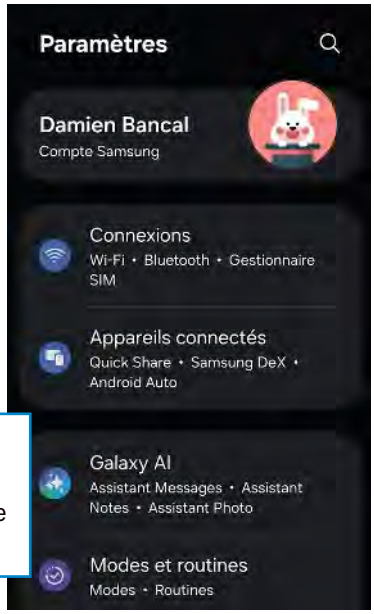
Fiche pratique

CHIFFRER SOUS ANDROID

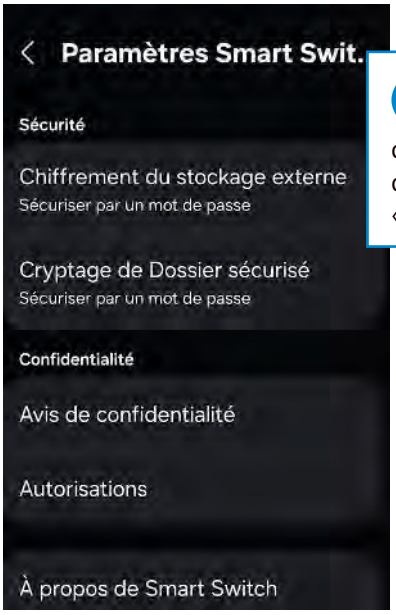
Chiffrer ses informations personnelles est un moyen quasi imparable de se protéger des regards non autorisés. Si vous possédez un smartphone sous Android, il est possible d'activer le chiffrement pour renforcer votre sécurité. Plusieurs méthodes existent, voici la plus courante (qui peut varier selon la version d'Android installée et le modèle de votre téléphone).



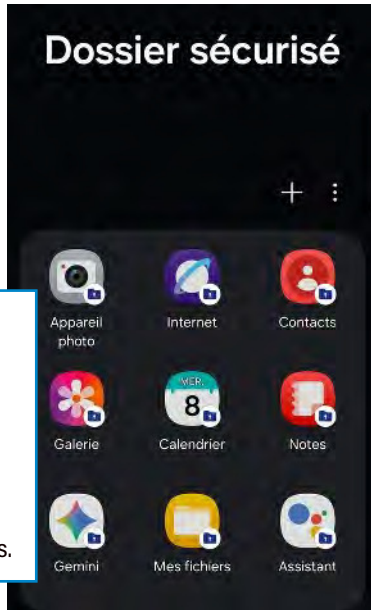
1 Avant tout, sauvegardez les données auxquelles vous tenez, car la mise en place du chiffrement peut supprimer des documents.



2 Chargez votre téléphone à 100 % pour éviter qu'il ne s'éteigne en plein processus.



3 Recherchez les paramètres de l'appareil, les options de sécurité et sélectionnez « Chiffrement du téléphone ».



4 N'oubliez pas de chiffrer la carte de stockage SD (celle de vos photos, par exemple), via l'option « Chiffrement du stockage ». Un mot de passe vous sera demandé pour déchiffrer vos contenus.

Smartphone ADOPTER UNE HYGIÈNE NUMÉRIQUE

Le mobile représente à présent une porte d'entrée géante sur notre vie privée. Y limiter l'accès à nos données personnelle est primordial pour se protéger. Nos conseils pour y parvenir.

Verrouiller son smartphone avec un mot de passe ou via la biométrie (reconnaissance faciale, empreintes digitales) empêche des personnes non autorisées d'accéder aux données qu'il contient. Un simple schéma de déverrouillage n'est, lui, pas recommandé, car plus facile à intercepter par un individu vous regardant le dessiner. Les mises à jour du téléphone, de son système d'exploitation et de ses applications sont aussi capitales pour la sécurité; ne les remettez pas à plus tard, car elles colmatent les potentielles brèches qu'exploiteraient les pirates.

Par ailleurs, activer l'option «Localiser mon appareil» est utile pour le retrouver en cas de perte ou de vol, mais aussi pour détruire son contenu à distance et/ou empêcher son utilisation. On ne le répétera jamais assez: se connecter à des wifi publics non sécurisés (proposés par des hôtels, des restaurants…) est dangereux, car ils sont vulnérables aux attaques d'escrocs qui eux aussi les utilisent… Quand on n'a pas d'autre choix que de s'y raccorder, il faut recourir à un réseau privé virtuel (VPN) pour sécuriser sa connexion (lire aussi p. 26 et p. 90). Il en existe de nombreux, mais attention ! Ceux mis en avant dans les publicités ne sont pas obligatoirement les meilleurs.

Applications et géolocalisation

Le bon réflexe, avec les applis, est de n'installer que celles provenant de sources fiables comme Google Play ou App Store. Des boutiques non officielles en proposent d'inédites, mais elles sont potentiellement dangereuses, car non contrôlées. Il faut d'ailleurs toujours s'interroger sur les autorisations sollicitées par une appli avant de la télécharger: certaines demandent un accès à des données sensibles (contacts, photos…), alors qu'elles n'en ont pas besoin ! Bref, à chaque fois, on fait du cas par cas. Pour cela, dans les réglages de son appareil puis dans «Applications», on configure les accès pour chacune, en les limitant aux moments où l'on s'en sert. À noter: certaines restrictions peuvent entraver leur bonne marche (par exemple, interdire la géolocalisation sur une appli de carte routière ou un GPS l'empêche de fonctionner). Il est possible, en revanche, d'imposer la fermeture des applis qui ne sont plus en service. Enfin, la vérification de leurs mises à jour importe aussi: chaque fois, des options peuvent apparaître comme disparaître (accès aux SMS, géolocalisation obligatoire, etc.).

Si le téléphone propose le chiffrement des données personnelles, on active cette option, car elle est protectrice en cas de vol ou de perte. Dans tous les cas, il faut éviter de stocker des informations

C'EST « MON » TÉLÉPHONE !

Au bureau, au resto, à la maison… votre téléphone a pu être visité, voire manipulé pour organiser à votre insu un renvoi d'appels, par exemple. Il faut vérifier… mais ne vous laissez pas séduire par les logiciels payants qui vous promettent de vous révéler un espionnage !

> **Le code *#21#,** que vous taperez sur le clavier de votre mobile, vous indiquera si un renvoi d'appels, de SMS ou de MMS a été mis en place.

> **Le code *#62#** vous fera connaître le numéro de redirection ; pour l'annuler, tapez ##002#.

sensibles (mots de passe, numéros de carte de crédit, captures d'écrans de carte d'identité…) sur son mobile, et le nettoyer (vider) très fréquemment. Le logiciel CCleaner pour téléphone portable peut s'en charger; le smartphone y gagnera en autonomie, en rapidité et en confidentialité.

Stocker fichiers et conversations

À ne pas négliger non plus, la sauvegarde régulière de ses fichiers sur un support de stockage externe, que l'on range ensuite dans un tiroir. Car, aussi pratiques que puissent être les clouds proposés par les constructeurs, ils demeurent des espaces extérieurs… et nos informations personnelles se retrouvent dehors. On veillera également à l'usage réservé aux données passant par le téléphone. Pour un modèle sous Android, il faut aller dans les options du wifi situé dans les « Réglages » de l'appareil. Sélectionnez alors « Utilisation des données » puis « Utilisation des données mobiles (ou wifi) » pour découvrir les applications les plus consommatrices d'informations personnelles. Pour un iPhone, il faut aller dans « Réglages > Données cellulaires ».
Intéressantes, certaines applications de messagerie sécurisent conversations et messages grâce au chiffrement de bout en bout. Parmi les meilleures, on trouve Olvid (France), Signal et Threema (Suisse) et WhatsApp (USA). Telegram pourrait être tentante (autodestruction des messages, chiffrement, etc.), mais ses origines russes, son siège social à Dubaï et les mystères qui entourent ses concepteurs, les frères Pavel et Nikolaï Durov, obligent à une retenue sécuritaire. Dans tous les cas, que la messagerie soit sécurisée ou non, il ne faut jamais cliquer sur des liens ou des pièces jointes provenant de sources suspectes. Enfin, pour une protection la plus efficace possible, le destinataire doit se servir de la même appli que l'émetteur.

UNE MESSAGERIE D'ÉTAT

À l'instar d'autres États européens, la France a adopté une messagerie instantanée qui s'appuie sur un protocole de chiffrement pour assurer la confidentialité des communications des agents de ses administrations, ministères ou armées. Baptisée Tchap et hébergée sur des serveurs du ministère de l'Intérieur, elle répond à des standards de sécurité nationale. Depuis septembre 2025, quelque 5 millions de fonctionnaires sont invités à utiliser cet outil « souverain », conçu par la Direction interministérielle du numérique (Dinum) et recommandé par l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Un iPhone n'est pas inviolable, mais il est considéré comme plus sûr.

PUTHITHON/ADOBE STOCK

L'iPhone est-il plus fiable ?

Même s'il n'est pas invulnérable, l'iPhone est considéré comme plus sûr que d'autres appareils. Apple est réputé pour la sécurité de ses modèles, en particulier en ce qui concerne la protection des données personnelles. L'une des raisons est la maîtrise totale du code source par le constructeur. Il est ainsi plus difficile pour des pirates de le perturber via des failles. Les mises à jour du système d'exploitation iOS, la capacité à installer uniquement des applications à partir de l'App Store, l'usage de la reconnaissance faciale et des technologies de chiffrement sont quelques-unes des mesures de sécurité classique de la marque à la pomme. Mais attention ! Aucun système n'est parfaitement sûr: les iPhone peuvent succomber à des attaques et leurs informations être volées, notamment par le biais d'applications malveillantes, de réseaux wifi publics ou de techniques d'hameçonnage (phishing). ■

Cybersécurité
LA TROUSSE DE SECOURS

On n'y pense pas toujours, mais une trousse de secours informatique peut nous sauver ! Voici la liste des huit outils de base.

1 L'ANTIVIRUS

Essentiel, un antivirus protège les appareils informatiques de toute la famille contre les virus, les logiciels malveillants et autres menaces en ligne. Plusieurs éditeurs – Avast, AVG, Avira, etc. – proposent des solutions gratuites efficaces, même si leurs fonctionnalités s'avèrent limitées. Par exemple, elles alertent si un virus se trouve dans un courriel, mais les options telles que la veille de votre ordinateur en temps réel, la protection contre les ransomwares («rançongiciels») et la correction des vulnérabilités des machines y demeurent souvent absentes.

2 L'ESPION 2.0

En complément d'un antivirus, pour découvrir si son appareil a été infecté, il est possible d'utiliser un «chasseur» de logiciels malveillants – du type cheval de Troie (programme informatique invasif et parfois destructeur) ou keylogger («enregistreur de frappes clavier»). Des outils gratuits tel AdwCleaner (Malwarebytes.com/fr) ou encore Spybot (Safer-networking.org) ont pour mission la recherche et la destruction de ceux cachés dans votre ordinateur. En général, on «attrape» un code malveillant quand on télécharge un logiciel par l'intermédiaire d'une source obscure et/ou non officielle.

3 LE FIREWALL

Ce dispositif de pare-feu va contrôler le trafic Internet entrant et sortant de l'ordinateur. Il analyse des «paquets» d'informations et bloque ceux considérés comme dangereux. À partir de la version 10 du système d'exploitation Windows, un firewall gratuit est intégré et activé par défaut (Windows Defender Firewall). Cette protection de base se révèle suffisante contre les connexions malveillantes qui tentent d'atteindre votre ordinateur. Parmi les autres solutions gratuites, GlassWire (aussi sur smartphone, Glasswire.com), TinyWall (Tinywall.pados.hu) ou encore ZoneAlarm Firewall, de l'éditeur Check Point (Zonealarm.com), sont recommandées.

4 LE VPN

Un réseau privé virtuel (VPN) chiffre le trafic internet de l'utilisateur et cache l'adresse IP de son ordinateur, ce qui rend plus difficile son identification. Des options gratuites comme Proton VPN (Protonvpn.com) ou bien TunnelBear (Tunnelbear.com) existent. Attention, elles sont limitées: leur vitesse de connexion ainsi que les protocoles de sécurité qu'elles emploient peuvent s'avérer moins robustes que ceux utilisés par les versions payantes. Sans parler des publicités récurrentes, fort pénibles à supporter…

5 LA SÉCURITÉ INTÉGRÉE ET LES EXTENSIONS

Les systèmes de navigation classiques comme Chrome, Edge, Firefox ou Opera disposent de fonctionnalités de sécurité natives, telles que la prévention des pop-up, le signalement de sites dangereux ou encore la protection contre les *trackers* (ces dispositifs qui mesurent les interactions des utilisateurs avec un site web ou toute autre forme de support électronique, et collectent des informations sur eux et leur environnement au moment de la consultation d'une page). Elles peuvent être renforcées par une «extension»,

Si investir dans certains outils aide à se protéger, intégrer les bonnes pratiques y contribue encore plus !

comme Adblock Plus ou encore Privacy Badger, l'outil créé par Electronic Frontier Foundation (Eff.org). Son but: bloquer les sites web qui tentent d'intercepter des renseignements sur les habitudes de l'internaute. Installer une extension de sécurité renforce aussi la sûreté du navigateur en l'obligeant, par exemple, à refuser tous les sites n'affichant pas https et le petit cadenas dans la barre d'adresse, signe d'une connexion sécurisée. C'est ce que proposait HTTPS Everywhere (aussi conçu par EFF) de 2010 à 2023, avant d'être abandonné, la Toile étant majoritairement passée au protocole https. Autre outil intéressant dans cette catégorie: NoScript (Addons.mozilla.org), qui empêche les scripts malveillants de se lancer à partir de pages infectées visitées. À savoir, toutefois: installer une extension peut perturber le fonctionnement de certains sites légitimes.

6 L'AUTHENTIFICATION À DEUX FACTEURS

Indispensable, l'authentification à deux facteurs (2FA) ajoute une «couche» de sécurité aux comptes en ligne en fournissant, par le biais d'une application, d'un SMS, d'un appel téléphonique ou d'un courrier électronique, une deuxième identification (second mot de passe, code, biométrie…). Il existe plusieurs dizaines d'applications en la matière, les plus utilisées étant Google Authenticator et Authy. Des clés USB spécifiques, dites FIDO U2F, proposent également la double authentification (Google Titan, Winkeo FIDO2, OnlyKey, YubiKey, etc.).

7 LA SAUVEGARDE ET LA SUPPRESSION

La sauvegarde régulière des données est incontournable, que ce soit sur un disque externe ou sur une clé USB – ne pas oublier de les tester avant pour ne pas se retrouver le bec dans l'eau le jour où l'on en a besoin. Auparavant, on aura fait du tri et opéré une suppression des fichiers devenus inutiles, d'autant que cela allège les supports de stockage, qui gagnent donc en rapidité. CCleaner ou Glary (Glarysoft.com) peuvent se charger de ce ménage. Notre coup de cœur ? L'outil gratuit BleachBit (Bleachbit.org), en open source, qui analyse et éradique les fichiers temporaires et inutiles, les caches ainsi que l'historique de navigation de l'ordinateur. Attention, un logiciel de suppression s'emploie avec du recul; certains fichiers importants pour la bonne marche de la machine ne doivent pas être jetés.

8 L'ADRESSE JETABLE

SimpleLogin (Simplelogin.io) propose de se créer une adresse électronique unique, destinée à une utilisation ponctuelle (pour participer à un concours en ligne, par exemple). Cela limite le risque de compromettre son compte de messagerie principal. ■

FLY AND DIVE/ADOBE STOCK

Osint UNE MINE D'INFOS

L'Osint, ou « renseignement en sources ouvertes », permet à n'importe qui de collecter ou de diffuser quantité d'informations grâce aux ressources offertes par Internet.

Les termes *open source intelligence,* ou Osint («renseignement en sources ouvertes») désignent l'exploitation d'informations publiques ou accessibles à tout un chacun (sites web, forums, journaux, bases de données, conférences, etc.) partout dans le monde, à des fins de renseignement. Mais il faut savoir que ce type de démarche remonte… à l'Antiquité ! De fait, les empereurs romains envoyaient déjà des espions récupérer des «tuyaux» sur les mouvements de l'ennemi. Ensuite et jusqu'au XV[e] siècle, les caravanes avançant sur la route de la soie, entre la Chine et Constantinople (Istanbul, en Turquie), servaient autant au commerce qu'à la collecte d'informations. Durant la Seconde Guerre mondiale, gouvernements, milices et résistants cherchaient tous à en savoir plus sur leurs adversaires pour mener ou parer des attaques. Ils ont donné à cette pratique un essor particulier en la portant jusqu'au zinc des bars… Quelques années plus tard, l'avènement de la guerre froide entre Russie et États-Unis la développera encore, puis Internet et les nouvelles technologies lui conféreront sa dimension actuelle, tentaculaire et mondiale.

Prenons l'exemple d'une simple photographie publiée sur le Web. Vous n'apercevez qu'un bout de la plaque d'immatriculation d'une voiture, une portion de route, deux bâtiments et des indications sur le sol, mais vous aimeriez bien savoir où le cliché a été pris ? GeoHints.com peut vous indiquer la marque du véhicule et sa géolocalisation en analysant la bordure du trottoir, les panneaux, les feux de signalisation, les poteaux électriques…

Même les étoiles parlent !

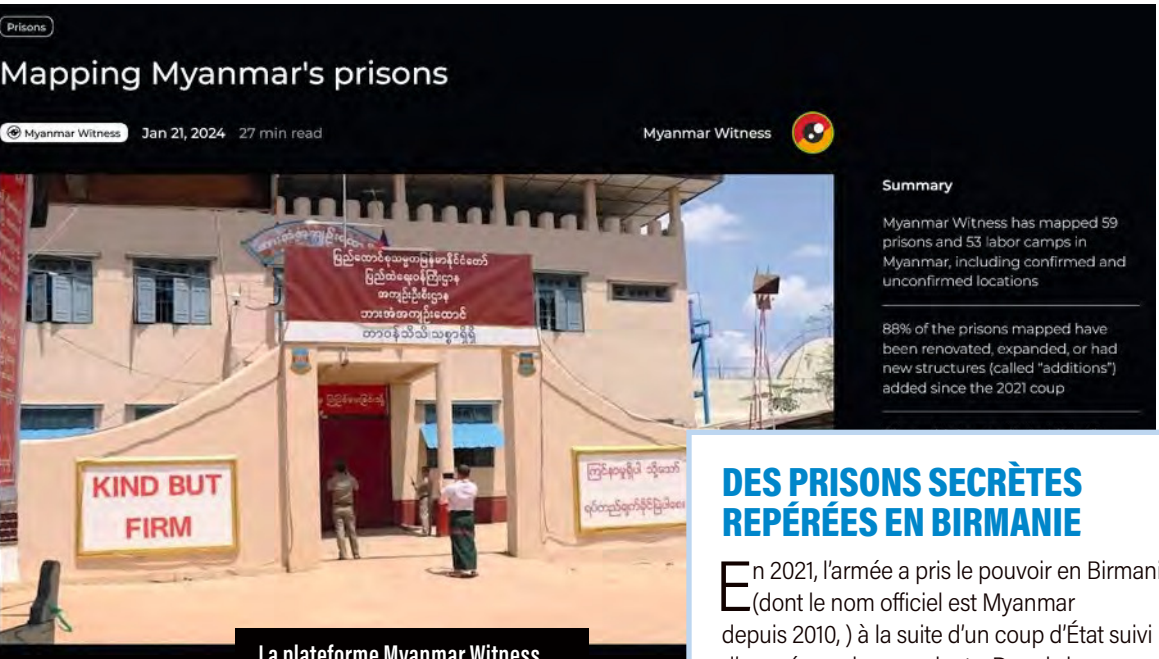
Le site Skyscraperpage.com s'est spécialisé, lui, dans la reconnaissance de toutes les tours érigées à travers le monde. Et Brueckenweb.de, dans celle des ponts. Les informations sont chaque fois regroupées dans des bases de données ouvertes et accessibles à tous. Il est ainsi devenu assez facile de situer la prise de vue d'une photo mystérieuse… Et, si elle a été faite durant la nuit et qu'on y voit des étoiles, il est même possible de retrouver ses coordonnées GPS, comme ce fut le cas avec un cliché d'un avion furtif B-21 de l'armée de l'air américaine. Le lieu de parking de ce bombardier a été découvert grâce à la position des étoiles, aux sites de passionnés d'astronomie et à Google Maps (source: Twitter.com/johnmcelhone8/status/1600683623250030593).

N'importe qui peut espionner

Il existe aujourd'hui des centaines de solutions pour collecter des informations à partir de sources ouvertes. Premiers de tous: les moteurs

DOCUMENTER LES CRIMES DE GUERRE

Eyes on Russia a été lancé par le Centre for Information Resilience (CIR) à la suite de l'invasion russe de l'Ukraine. Il mobilise une communauté Osint internationale pour répertorier les atrocités commises. Grâce à l'usage intensif d'images satellites, d'analyse de vidéos, de témoignages et de données géolocalisées, les enquêteurs ont pu suivre les déplacements de troupes, recenser les dommages aux infrastructures et enregistrer plus de 23 000 incidents, parmi lesquels des déportations d'enfants, des détentions illégales, de la torture et des exécutions ciblées. Ces preuves détaillées sont mises en ligne notamment sous la forme d'une carte interactive, afin de documenter les crimes de guerre et de responsabiliser leurs auteurs. Consultable sur le site du CIR, Info-res.org/eyes-on-russia.



La plateforme Myanmar Witness révèle, entre autres, l'expansion de la détention politique en Birmanie.

de recherche. Leur fonctionnalité de base – trouver rapidement des données depuis des mots-clés – en fait de précieux alliés. Viennent ensuite les réseaux sociaux. Facebook, Instagram, LinkedIn ou Twitter sont de vraies pipelettes ! Ils permettent de se renseigner sur les activités de leurs abonnés, leurs centres d'intérêt, leur emploi du temps, leurs vacances, etc. En outre, les solutions de cartographie telles Google Maps ou Bing Maps, fournissent des données sur les lieux, les bâtiments, les routes et les itinéraires. Bref, autant d'instruments que les espions de la guerre froide auraient pu nous envier.

Citons trois autres outils. Le premier, Google Alerts (Google.com/alerts), est un service gratuit grand public qui permet de définir des mots-clés de recherche et de recevoir des notifications dès que de nouveaux contenus y correspondant sont publiés sur Internet. Idéal pour suivre l'actualité sur un thème précis ou être prévenu si son identité apparaît quelque part, sa couverture des réseaux sociaux n'est toutefois pas poussée. Le second, Social Searcher (Social-searcher.com), surtout utilisé par les professionnels, sert à scruter les réseaux sociaux, blogs et forums, et propose une veille gratuite de l'e-réputation d'une marque ou d'un service. Enfin le troisième, intitulé Mention (Mention.com) est destiné essentiellement aux entreprises et aux spécialistes du marketing. Il offre une surveillance complète du Web et une analyse avancée (sentiment, influence, rapports…) de la présence en ligne. ■

DES PRISONS SECRÈTES REPÉRÉES EN BIRMANIE

En 2021, l'armée a pris le pouvoir en Birmanie (dont le nom officiel est Myanmar depuis 2010,) à la suite d'un coup d'État suivi d'une répression sanglante. Depuis lors, le pays est le théâtre de multiples violations des droits de l'homme. Malgré l'opacité imposée par la junte militaire, la plateforme Myanmar Witness, reposant sur l'Osint, a pu les révéler. Elle permet en effet aux Birmans de diffuser, après authentification par des experts, des preuves (photos, vidéos…) d'atteintes aux libertés, de façon anonyme afin d'éviter les représailles. Ce projet de collecte, d'analyse et de vérification des informations a notamment servi à documenter l'expansion du système carcéral birman. À partir d'images satellites, de rapports publics et de témoignages, plus de 100 prisons et camps de travail ont été identifiés, dont une moitié a été agrandie après la prise du pouvoir par les militaires… Deux nouveaux complexes, à Mawlamyine et dans l'État d'Ayeyarwady, ont même été découverts. Ces données recoupent les alertes sur la hausse des détenus politiques et les abus.

CAPTURE D'ÉCRAN

Se faire aider

Si vous découvrez que vous êtes victime d'une cyberattaque, la priorité absolue est de vous protéger rapidement et de solliciter de l'aide, afin d'éviter que ce piratage ne vire au cauchemar. Ressentir de la honte ou de l'embarras est fréquent, mais rappelez-vous que personne n'est à l'abri. Les cybercriminels perfectionnent sans cesse leurs méthodes: faux sites, hameçonnage, arnaques bancaires… Leurs attaques sont devenues si sophistiquées qu'elles trompent même les internautes les plus prudents. La bonne réaction en cas de problème? Alerter immédiatement les autorités. Dans ce chapitre, vous trouverez les principaux sites et plateformes d'assistance à contacter, ainsi que les conseils de prudence de Myriam Quéméner, une référence en droit numérique en France.

SOMMAIRE

EXENTIA/ADOBE STOCK ; TALAJ/ISTOCK

Récupération SUR LA TRACE DES DONNÉES PERDUES

Ce moment de panique quand nous réalisons avoir supprimé des fichiers importants de notre ordinateur, de notre téléphone ou de notre clé USB… Beaucoup d'entre nous ont vécu cette mauvaise expérience. Mais restons zen ! Il existe des solutions.

Lorsque l'on perd des données, c'est très souvent par accident. Le premier geste fâcheux qui fait disparaître un document, mais qui est, fort heureusement, rattrapable ? La suppression malencontreuse d'un fichier, qui atterrit alors à la poubelle. Par chance, l'en ressortir suffit à corriger l'erreur. Sur PC, il faut cliquer en même temps sur CTRL + Z; sur Mac, c'est Command + Z. Seconde cause de perte, qui n'est pas non plus définitive : le déplacement intempestif, soit un «glissé» malheureux qui conduit votre document à disparaître dans les méandres de l'ordinateur. Ne paniquez pas, la commande proposée plus haut viendra à votre secours. D'autres situations se révèlent cependant plus dramatiques, comme le formatage accidentel: vous êtes en train de formater votre support numérique quand, tout à coup, vous vous rendez compte que vous n'avez pas sauvegardé des données essentielles. Et c'est trop tard… N'oublions pas également la panne matérielle et l'écrasement de fichiers, la prise en otage de ces derniers par un code malveillant (rançongiciel, cryptolocker), ou encore l'attaque d'un virus qui les détruit ou les endommage.

RÉCUPÉRER LES DONNÉES DISPARUES SUR UN ORDINATEUR

Plusieurs logiciels gratuits sont capables d'aider à retrouver des données effacées. Toutefois, attention: si vous vous rendez compte de l'erreur fatale, stoppez tout usage du support de stockage, afin d'éviter d'écraser vos documents avec d'autres fichiers. Parmi les solutions gratuites, citons Recuva, de Piriform (la société qui édite CCleaner), EaseUS Data Recovery Wizard ou TestDisk, un outil open source. Une fois installé sur votre poste, le logiciel de récupération vous propose de scanner le support de stockage (autrement dit, de lire son contenu) à partir duquel les données ont été supprimées, afin de rechercher les fichiers perdus. Une fois l'analyse terminée, l'outil vous indique ce qu'il est possible de sauver. Attention, selon la taille et le type de document (texte, image, vidéo), la récupération risque d'être partielle.

RETROUVER DES FICHIERS EFFACÉS D'UN SMARTPHONE

La complexité d'un mobile de nouvelle génération, véritable «ordiphone», laisse peu de chances à son propriétaire de récupérer un fichier, une photo ou une vidéo effacée. S'il s'agit d'un appareil sous Android, des outils comme Dr Fone, DiskDigger, EaseUS MobiSaver ou Recuva annoncent pouvoir vous aider. Il est cependant important de comprendre que retrouver des données n'est absolument pas garanti. Par sa nature, le smartphone enregistre en permanence des informations; la récupération peut donc ne pas être possible en raison d'une écriture massive. L'outil écrit des dizaines de fois la même chose (des lignes de chiffres et de lettres aléatoires) sur les mêmes fichiers… Sur un téléphone portable, la meilleure méthode pour ne pas perdre ses données, c'est de les sauvegarder très régulièrement.

CONTRÔLER LES RÉSEAUX SOCIAUX

Vous êtes en mesure de collecter l'ensemble des éléments que vous avez diffusés sur un réseau social depuis votre inscription. Chaque

Un clic trop rapide, et le travail de la journée peut s'envoler... Prenez vos précautions en amont pour le récupérer.

plateforme possède ses propres fonctionnalités de récupération d'archives et de données (sauf Snapchat). Nous vous indiquons ci-dessous celles à connaître sur deux des réseaux sociaux les plus populaires, Facebook et Instagram.

Connectez-vous à votre profil Facebook ou Instagram sur l'ordinateur. Allez dans votre compte (votre photo en haut, à droite) et cliquez sur «Paramètres et confidentialité» puis dans «Paramètres». Dans la colonne de gauche, écrivez «Vos informations et autorisations» dans le petit moteur de recherche. Cliquez sur «Exporter vos informations» puis sur «Créer une exportation». Choisissez ensuite le compte à sauvegarder (Facebook, Instagram ou l'ensemble des données détenues par Meta, la maison mère des deux réseaux sociaux). Sélectionnez «Exporter sur mon appareil».

Dans la fenêtre «Confirmer votre exportation», apparaît l'onglet «Avertir» avec l'adresse électronique de réception du lien de téléchargement. En dessous, dans «Personnaliser les informations», décochez les options qui ne vous intéressent pas parmi les 55 proposées. De nouveau, plus bas, indiquez la «Période», le «Format» de réception (HTML conseillé) et la «Qualité des contenus multimédias» – la durée de sauvegarde dépendra de la résolution des images. Cliquez sur «Commencer l'exportation». Vous recevrez ensuite un e-mail vous indiquant quand vous pouvez télécharger vos archives. Plus la demande est importante, plus le délai est long (jusqu'à 15 jours). ■

LE TOP 3 DES OUTILS POUR RETROUVER DES FICHIERS SUPPRIMÉS

> **TestDisk** est un logiciel de récupération de données gratuit. Il peut retrouver des fichiers perdus à partir de disques durs, même endommagés, de cartes mémoire ou de clés USB. Pas particulièrement convivial, il se montre cependant très efficace. Cet outil est disponible sur les systèmes d'exploitation Windows, Mac et Linux.
Cgsecurity.org/wiki/TestDisk_FR

> **Recuva** est gratuit et facile à utiliser. Il peut retrouver des fichiers supprimés de la corbeille, perdus après un formatage de disque dur et même ceux disparus à la suite d'erreurs système. Il est disponible pour les ordinateurs sous MacOS et Windows. Il existe une version payante avec de nombreuses options.
Ccleaner.com/fr-fr/recuva/download

> **PhotoRec** appartient à la famille TestDisk. Sa spécialité ? Retrouver des images qui étaient stockées dans les mémoires d'appareils photos. Vous avez formaté votre carte SD ? Vos clichés et vos vidéos pourront être collectés. Mais attention, ne sauvegardez plus aucun fichier sur le support avant de lancer une procédure de récupération.
Cgsecurity.org/wiki/PhotoRec_FR

INFINITEFLOW/ADOBE STOCK

Interview

MYRIAM QUÉMÉNER Ancienne magistrate, spécialiste des nouvelles technologies et de la cybercriminalité

« PROTÉGER NOS DONNÉES EST AUSSI UN ENJEU DÉMOCRATIQUE »

Magistrate depuis 1986, docteure en droit et spécialiste de la cybercriminalité, Myriam Quéméner a exercé des responsabilités de premier plan aux ministères de la Justice et de l'Intérieur ainsi qu'à la cour d'appel de Versailles. Elle nous livre son analyse des enjeux qui redessinent notre société numérique.

QC Pourquoi la protection des données personnelles est-elle un enjeu majeur pour les citoyens comme pour les entreprises ?

Myriam Quéméner Les données numériques constituent un véritable patrimoine informationnel. S'agissant des entreprises, elles représentent non seulement un actif économique, mais également un levier stratégique face à la concurrence. Dans un contexte politique, financier et géopolitique tendu, leur protection est essentielle, afin de garantir la souveraineté numérique et la confiance des partenaires. En ce qui concerne les citoyens, la question est tout aussi vitale. La fuite ou le vol de données peut entraîner des usurpations d'identité, des fraudes bancaires et un préjudice psychologique durable. Les cybercriminels exploitent les failles humaines et techniques pour monnayer ces informations sur des marchés parallèles.

QC Quelles sont les erreurs les plus fréquentes que nous commettons avec nos informations personnelles en ligne ?

M. Q. La négligence reste le principal facteur de vulnérabilité. Beaucoup de personnes cliquent encore sur des liens ou des pièces jointes provenant d'e-mails suspects. L'absence de mises à jour régulières sur les appareils constitue également un point critique. On observe aussi des mots de passe trop faibles ou réutilisés sur plusieurs services, ainsi qu'un partage excessif d'informations personnelles sur les réseaux sociaux, ce qui facilite l'ingénierie sociale.

QC Comment expliquer au grand public que nos données, c'est notre identité numérique ? En quoi leur perte et leur vol peuvent-ils nous impacter ?

M. Q. Il faut insister sur le fait que les données personnelles sont le reflet de notre identité: adresse, numéro de Sécurité sociale, habitudes de consommation, données médicales, photos… Si elles sont compromises, c'est toute une vie qui risque de basculer. Une usurpation peut bloquer un crédit, ruiner une réputation ou exposer une intimité. La pédagogie doit commencer dès le plus jeune âge, à l'école, afin d'ancrer les bons réflexes – comme on l'a fait autrefois avec la sécurité routière.

QC Avec l'essor du *big data* et de l'intelligence artificielle (IA), nos données sont massivement collectées et analysées. Faut-il s'inquiéter d'une perte de contrôle ?

M. Q. Oui, car l'accumulation de données alimente des systèmes d'IA capables de profiler les individus avec une précision inédite. Le risque est de voir émerger une société de surveillance où nos comportements sont prédits, influencés et parfois manipulés.

L'enjeu n'est pas seulement individuel, il est aussi démocratique: protéger les données, c'est protéger les libertés fondamentales.

Q C La Cnil[1] et le RGPD[2] donnent un cadre légal. Mais cela suffit-il face à des cybercriminels toujours plus inventifs ?

M. Q. Le RGPD constitue un socle essentiel, mais il doit être complété par d'autres normes, comme NIS 2, Dora ou le Cyber Resilience Act (CRA). Ces textes renforcent la sécurité des infrastructures critiques, des services financiers et des produits numériques. Toutefois, au-delà du droit, il faut des moyens: l'État doit accompagner les entreprises, en particulier les PME, pour leur permettre d'instaurer une vraie conformité technique et organisationnelle.

Q C Quels conseils concrets prodigueriez-vous à un particulier pour mieux protéger ses données au quotidien, sans tomber dans la paranoïa numérique ?

M. Q. Adoptez la mise à jour régulière des appareils; l'emploi de mots de passe robustes et d'un gestionnaire dédié ; l'authentification à deux facteurs. Soyez méfiants envers les messages suspects et vérifiez l'authenticité des expéditeurs; limitez les informations partagées publiquement. La vigilance n'exclut pas la curiosité. Se former et s'informer permet d'agir sans céder à la peur.

Q C La cybersécurité est souvent perçue comme technique. Comment la rendre plus accessible au grand public ?

M. Q. En la vulgarisant. Beaucoup d'initiatives existent: le Cybermois en octobre, les campagnes de sensibilisation dans les écoles, une coopération public-privé en constante évolution. Il faut parler de cybersécurité comme on parle d'hygiène… Se laver les mains paraît évident, protéger ses données doit le devenir tout autant.

Q C Selon votre expérience internationale, notamment acquise auprès du Conseil de l'Europe, la protection des données est-elle perçue et traitée de la même manière partout dans le monde ?

M. Q. Non, la protection des citoyens est inégale. Certains pays considèrent leurs données comme une ressource stratégique et n'hésitent pas à les exploiter de façon prédatrice, dans un climat de concurrence exacerbée. C'est souvent la «loi de la jungle». À l'inverse, l'Union européenne a construit un corpus juridique exigeant, qu'elle impose aux acteurs étrangers souhaitant commercer sur son marché. Cela lui confère un rôle de régulateur mondial.

Q C Comment voyez-vous l'avenir de la protection des données dans 10 ans ? Quels défis majeurs faudra-t-il relever ?

M. Q. La protection des données devra être intégrée dans l'ADN de chaque organisation et dans la culture de chaque citoyen. Dans 10 ans, les défis seront multiples: sécuriser les objets connectés omniprésents, encadrer l'intelligence artificielle, maîtriser la souveraineté des infrastructures cloud, protéger les données de santé, renforcer la résilience face aux cyberattaques étatiques… C'est une condition de survie pour les sociétés, et de confiance pour nos démocraties. ■

(1) Commission nationale de l'informatique et des libertés.
(2) Règlement général sur la protection des données.

Assistance
LES ADRESSES UTILES

Comment réagir face à une fuite de données ou un assaut informatique ? Des plateformes peuvent vous aider. Enregistrez-les dans vos favoris.

ANSSI

L'Agence nationale de la sécurité des systèmes d'information fournit des conseils et une assistance aux particuliers et aux entreprises. Elle assure aussi des formations pour sensibiliser aux bonnes pratiques, ainsi que des audits de sécurité afin d'évaluer les vulnérabilités des systèmes. L'adresse à enregistrer: **Cyber.gouv.fr.**

BRIGADE NUMÉRIQUE

La Brigade numérique de la gendarmerie nationale, créée en 2018, est disponible 24 h/24 et 7 j/7 via un tchat en ligne. On peut y échanger avec un gendarme pour signaler une fraude, poser des questions ou obtenir de l'aide face au cyberharcèlement et aux usurpations d'identité. L'adresse à enregistrer: **Gendarmerie.interieur.gouv.fr.**

CNIL

La Commission nationale de l'informatique et des libertés (Cnil) est une autorité administrative indépendante. Elle a été mise en place pour protéger la vie privée et les données personnelles des citoyens. Sa plateforme les renseigne sur leurs droits et publie des recommandations pour se prémunir contre les atteintes sur Internet. L'adresse à enregistrer: **Cnil.fr.**

CYBERMALVEILLANCE.GOUV.FR

Cette plateforme offre une assistance gratuite aux internautes et la possibilité de déclarer les actes délictueux dont ils ont été victimes. Elle donne des conseils et des solutions pour y faire face. Une mise en relation (payante) avec des entreprises privées est permise. L'adresse à enregistrer: **Cybermalveillance.gouv.fr.**

E-ENFANCE

Reconnue d'utilité publique, l'association e-Enfance assure une mission de protection des jeunes sur Internet, et d'éducation à la citoyenneté numérique. Sur son site, les parents peuvent, entre autres, trouver des conseils pour protéger

LES BONS RÉFLEXES

Dirigeant d'une PME/PMI, vous êtes détenteur d'un savoir-faire unique. Derrière une attaque informatique contre votre société, peut se cacher un acteur hostile ou malveillant qui vise non seulement l'espionnage industriel, mais aussi la désinformation, le sabotage, la perturbation du fonctionnement de votre entreprise ou l'exfiltration de données. Au moindre doute, alertez la Direction générale de la sécurité intérieure (DGSI). Contact sur Dgsi.interieur.gouv.fr.

Cybermalveillance.gouv.fr sert à signaler les actes délictueux en ligne.

LES 7 ACTIONS À MENER

Vous venez de subir d'une attaque numérique ? Voici ce qu'il faut faire.

1 **Alertez immédiatement votre banque** en cas de fuite de vos données bancaires (à la suite d'un hameçonnage, notamment).

2 **Gardez toutes les preuves** (captures d'écran, tchats, courriels, etc.).

3 **Déposez une plainte** auprès de la police ou de la gendarmerie.

4 **Contactez le service fraude** de votre banque et l'ambassade locale si vous êtes à l'étranger.

5 **Signalez les actes de malveillance pour éviter toute usurpation** pouvant impacter votre famille et/ou vos collègues.

6 **Débranchez votre ordinateur d'Internet** s'il a été infiltré.

7 **Changez vos mots de passe** à partir d'un appareil sain.

leur progéniture des pièges du Web. Surtout, elle offre une assistance aux enfants et aux adolescents victimes de cyberharcèlement, grâce au numéro court et à l'application 3018. L'adresse à enregistrer: **E-enfance.org.**

INFO-ESCROQUERIES

Née en 2009, la plateforme téléphonique Info-Escroqueries du ministère de l'Intérieur fournit des clés de compréhension des différentes formes d'arnaques en ligne. Elle permet aux particuliers de signaler les actes de malveillance qu'ils ont subis et d'apprendre les bons gestes pour se protéger. Si vous souhaitez la joindre, composez le 0 805 805 817 (service et appel gratuits), du lundi au vendredi, de 9 h à 18 h 30.

MA SÉCURITÉ

Le ministère de l'Intérieur a créé un site (ex-Moncommissariat.fr) pour délivrer des informations utiles: annuaire des commissariats et des gendarmeries, fiches pratiques sur les arnaques, etc. Policiers et gendarmes y accompagnent chacun dans ses démarches. Sur la page d'accueil, un onglet fait accéder au service de Traitement harmonisé des enquêtes et signalements pour les e-escroqueries (Thesee) et permet de déposer plainte. L'adresse à enregistrer: **Masecurite.interieur.gouv.fr.**

PLAINTE EN LIGNE

Ce service ministériel sert à effectuer une déclaration pour des faits d'atteinte aux biens (vols, dégradations, escroqueries…) dont on peut être victime et pour lesquels on ne connaît pas l'identité de l'auteur. L'adresse à enregistrer: **Plainte-en-ligne.masecurite.interieur.gouv.fr.**

PHAROS

Créée par le ministère de l'Intérieur, la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) est dédiée à la lutte contre les propos ou les comportements illégaux sur Internet. Elle propose également une assistance aux victimes de délit informatique. L'adresse à enregistrer: **Internet-signalement.gouv.fr.**

POINT DE CONTACT

Lancée par l'Union européenne, cette plateforme permet aux internautes de signaler anonymement les contenus illicites ou choquants (appel au terrorisme, pédopornographie, etc.) qu'ils découvrent sur Internet. L'outil existe sous deux formes, un module pour navigateur web et une application mobile. L'adresse à enregistrer: **Pointdecontact.net.**

SIGNAL SPAM

Cette plateforme sert à signaler les messages indésirables reçus par courriel (dits spams) ou par SMS/MMS. Des sociétés privées se chargent ensuite d'alerter leurs clients. Les signalements sont aussi communiqués aux autorités afin de lutter contre ces pratiques illégales. L'adresse à enregistrer: **Signal-spam.fr.**

17CYBER

Ce dispositif de lutte contre la cybermalveillance combine la technologie (diagnostic en ligne) avec l'expertise humaine (forces de l'ordre) pour protéger et accompagner ceux qui en ont besoin face à la délinquance informatique. L'adresse à enregistrer: **17cyber.gouv.fr.** ■

DÉJOUER **LES ATTAQUES**

Différentes options s'offrent à vous pour protéger votre ordinateur. Antivirus intégré à Windows ou solution tierce ? Logiciel gratuit ou payant ? Nos conseils.

Les pirates ne manquent pas d'imagination. Chaque année, des millions de nouveaux logiciels malveillants apparaissent: les espions, qui récupèrent les informations de votre ordinateur; les chevaux de Troie, conçus pour prendre son contrôle, les rançongiciels qui bloquent votre machine jusqu'au paiement d'une rançon (si ça vous arrive, ne versez rien !). S'y ajoutent les tentatives de phishing (hameçonnage) visant à récolter vos données personnelles… Sur les Mac, le risque d'être infecté par un malware est faible, mais sur PC, avoir un antivirus reste une sage précaution.

Nous avons testé 11 solutions non seulement pour vérifier leur efficacité et leur facilité d'utilisation, mais aussi pour comprendre les différences entre les options gratuites et payantes. Le premier constat est plutôt rassurant: leurs performances suffisent à la plupart des usages. Le deuxième l'est un peu moins puisqu'aucun logiciel n'est absolument infaillible. Les antivirus arrêtent parfois par erreur des fichiers anodins et en laissent passer d'autres, virulents. Pas de quoi, cependant, remettre en cause leur utilité. En plus de la protection qu'ils offrent face aux attaques informatiques, nous avons vérifié qu'une fois installés, les antivirus n'impactent pas les performances de votre ordinateur. Comme tout logiciel, ils consomment des ressources (espace sur le disque dur, mémoire vive) et sollicitent le processeur pour l'exécution de leurs tâches. Ainsi, certains occupent jusqu'à 3 Go sur le disque dur.

GUVENDEMIR/ISTOCK

Les options annexes

Vous constaterez, dans notre tableau, que les suites payantes ne se montrent pas plus performantes que les gratuites. Dès lors, pourquoi dépenser de l'argent ? En fait, les premières proposent des services annexes: *virtual private network* (VPN) qui protège votre connexion à Internet, pare-feu propriétaire, gestionnaire de mots de passe, contrôle parental, sauvegarde en ligne, etc.

Notez, au passage, que les caractéristiques des VPN diffèrent d'un éditeur à l'autre. S'il est pleinement fonctionnel, sans restriction de données chez Norton et McAfee, il est limité à 1 Go quotidien chez Avira. Ce dernier, en version payante, propose l'analyse des pièces jointes des courriels et un outil pour vérifier la sécurité du réseau, ainsi qu'un accès illimité au service client. Ces fonctions permettent surtout aux marques de se distinguer les unes des autres et de convertir les utilisateurs d'une solution gratuite à la version payante. Notre suivi régulier de ces logiciels révèle par ailleurs que ces fonctionnalités vont et viennent au gré de l'éditeur: il n'est pas impossible qu'elles disparaissent sans préavis. Pour un service de sauvegarde en ligne ou un gestionnaire de mots de passe, mieux vaut choisir une offre dédiée (lire aussi p. 38-41 et p. 62-65). ■

Test

11 SOLUTIONS GRATUITES ET PAYANTES ANALYSÉES

★★★ très bon ★★ bon
★ moyen ■ médiocre
■■ mauvais ● oui - non

		Facilité d'emploi				NOTE SUR 20	APPRÉCIATION	PRIX (1) €	Pare-feu propriétaire	Gestionnaire de mots de passe	Sauvegarde en ligne (cloud fabricant)	VPN	Contrôle parental
		PROTECTION	INSTALLATION ET DÉSINSTALLATION	IMPACT SUR LES PERFORMANCES DU PC	UTILISATION								
1	**AVIRA** INTERNET SECURITY	★★★	★★	★★★	★★	**17,1**	★★★	65	●	●	-	●	-
2	**G DATA** INTERNET SECURITY	★★★	★★	★★★	★★★	**17**	★★★	56	●	-	-	-	●
3	**NORTON** 360 STANDARD	★★★	★★	★★★	★★★	**17**	★★★	75 (2)	●	●	●	●	-
4	**AVIRA** FREE SECURITY	★★★	★★	★★★	★★	**16,9**	★★★	Gratuit	-	●	-	●	-
5	**BITDEFENDER** INTERNET SECURITY	★★★	★★	★★	★★★	**16,8**	★★★	65	●	-	-	●	●
6	**BITDEFENDER** ANTIVIRUS FREE	★★★	★★	★★	★★★	**16,8**	★★★	Gratuit	-	-	-	●	-
7	**MCAFEE** TOTAL PROTECTION	★★★	★★	★★★	★★★	**16,8**	★★★	110 (3)	●	-	-	●	-
8	**ESET** HOME SECURITY ESSENTIAL	★★★	★★★	★★★	★★★	**16,5**	★★★	60	●	-	-	-	●
9	**F-SECURE** INTERNET SECURITY	★★★	★★	★★★	★★	**16,4**	★★★	70	-	-	-	-	●
10	**TREND MICRO** INTERNET SECURITY	★★	★★	★★	★★	**14,1**	★★	60	-	-	-	-	●
11	**MICROSOFT** DEFENDER (4)	★	★★★	★★★	★★	**11,7**	★	Gratuit	-	-	-	-	-

(1) Prix pour une licence d'un an et trois appareils, fournis à titre indicatif. Ils peuvent varier considérablement, notamment la première année, au gré des promotions. (2) Licence un appareil. (3) Licence cinq appareils. (4) Intégré à Windows 10 et 11.

NOTRE MÉTHODE

Nos tests évaluent la capacité des antivirus à protéger un ordinateur. **Nous visitons** 100 sites hébergeant des fichiers malveillants, connectons une clé USB infectée et stockons 10 000 fichiers (troyens, virus, espions) sur le PC. **Nous vérifions** ensuite la facilité d'utilisation du logiciel (installation, désinstallation, espace occupé, rapidité d'exécution, etc.).

USERBA011D64/ISTOCK

Le meilleur

Avira

Avira INTERNET SECURITY
65 € **17,1/20** | ★★★

Avira fait coup double : ses deux outils, payant et gratuit, obtiennent des notes très proches. Les applications offrent un excellent niveau de protection contre les fichiers malveillants et contre les sites de phishing, par le biais d'une extension à installer dans le navigateur. La version payante comporte l'analyse des pièces jointes aux e-mails ou un accès illimité au service client.

L'alternative

Bitdefender

Bitdefender ANTIVIRUS FREE
Gratuit **16,8/20** | ★★★

Cette version gratuite donne les mêmes protections de base (antivirus avec suivi comportemental et antiphishing) que la payante. Les deux sont efficaces. Seuls quelques rares fichiers et sites anodins ont été bloqués par erreur et 85 % des sites d'hameçonnage ont été repérés. L'installation est simple, et le logiciel impacte relativement peu les performances de l'ordinateur.

Mini-guide *Antivirus*

INSTALLER ET CONFIGURER **AVIRA INTERNET SECURITY**

- **Objectif :** profiter du meilleur outil de protection payant.
- **Niveau de difficulté :** facile. **Temps nécessaire :** 10 à 15 minutes.

CHOISIR LA BONNE FORMULE

La suite gratuite (Avira Free Security, aussi testée, lire tableau p. 103) se contente d'un antivirus et d'un VPN. La version payante, Avira Internet Security, dispose, elle, de nombreuses fonctionnalités: l'analyse des pièces jointes des courriels, un outil qui vérifie la sécurité du réseau, ou encore un accès illimité au service client. Elle coûte 65 € pour une licence d'un an et trois ordinateurs sous Windows (sans offre promotionnelle la première année). Si vous n'avez qu'un PC, préférez la licence monoposte, à 27 € la première année, puis à 55 €. Vous voulez protéger plusieurs types d'appareils (iOS, MacOS, Windows, Android) avec une seule licence? Optez pour la version multiplateforme Avira Prime.

UNE PROTECTION EFFICACE CONTRE LES MENACES

L'installation ne pose aucun problème. Une fois le paiement effectué sur le site de l'éditeur du logiciel, ce dernier vous invite à cliquer sur «Installer maintenant» pour lancer le process. Vous serez ensuite pris par la main (image 2). L'antivirus occupe environ 1 Go d'espace sur votre ordinateur, ce qui est raisonnable, certaines solutions s'octroyant jusqu'à 3 Go. Notre test montre qu'Avira Internet Security protège efficacement le PC contre les sites et les fichiers malveillants, avec peu de faux positifs (erreurs d'appréciation du logiciel). La protection contre l'hameçonnage fonctionne via une extension à installer dans le navigateur et se révèle assez efficace, avec 89 % de sites bloqués.

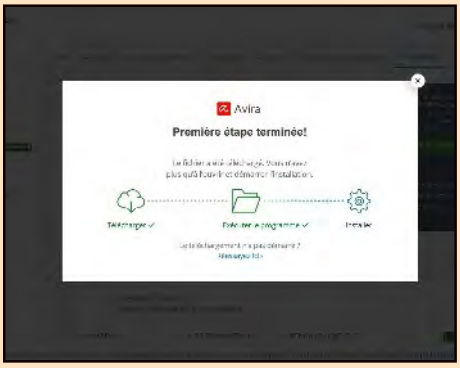
UN USAGE INTUITIF

À la première utilisation, vous pourrez lancer un scan de votre PC afin d'établir un premier diagnostic des anomalies (image 4). L'analyse de fichiers risque d'être assez lente mais, en cas de détection d'une menace, les alertes sont suffisamment explicites. En plus d'être simple à installer et performante, cette suite offre une bonne ergonomie. Dans l'interface, les menus sont organisés sur la gauche de l'écran, par onglet selon le type de fonctions (image 5). «Sécurité» permet de piloter le scan de virus, d'activer et désactiver les protections, d'examiner les fichiers en quarantaine s'il y en a, d'observer l'activité du pare-feu (trafic réseau). «Confidentialité» regroupe un VPN [Virtual Private Network, ou réseau privé virtuel, pour naviguer sur Internet en cachant l'adresse de votre appareil], un gestionnaire de mots de passe et un bloqueur de publicités, très appréciable quand on surfe sur le Web. Enfin, derrière l'onglet «Performances», vous trouverez tous les réglages permettant d'optimiser le fonctionnement de votre ordinateur (économiseur de batterie, détection de fichiers stockés en double, etc.). ■

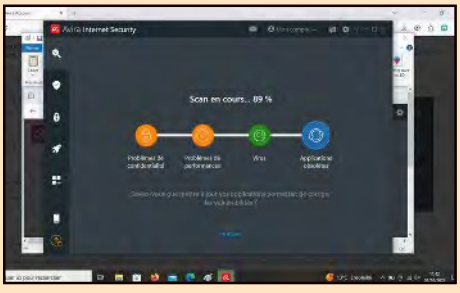
Bon à savoir

Les systèmes d'exploitation Windows 10 et 11 intègrent d'office les protections indispensables que sont l'antivirus et le pare-feu, et c'est... gratuit ! Cependant, les nombreuses fonctionnalités des solutions payantes sont appréciables. Certaines d'entre elles comportent un gestionnaire de mots de passe, un VPN, voire un destructeur de fichiers.

1 L'abonnement à Avira Internet Security est proposé pour un mois, un an ou deux ans, souvent avec des prix dégressifs. Vous pourrez sélectionner le nombre d'appareils que vous souhaitez protéger. Attention, à échéance, l'abonnement se renouvelle automatiquement. Pour le stopper, il faut l'annuler un mois avant.

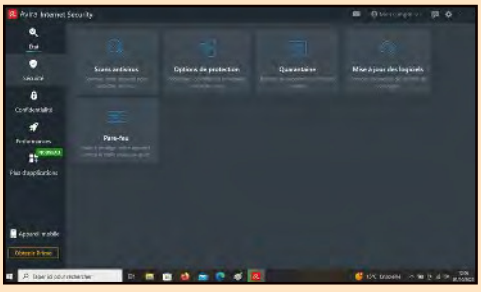


2 Après le paiement, vous serez pris par la main afin de définir un mot de passe et d'installer le logiciel. Une flèche rouge explicite vous indique où vous devez cliquer.

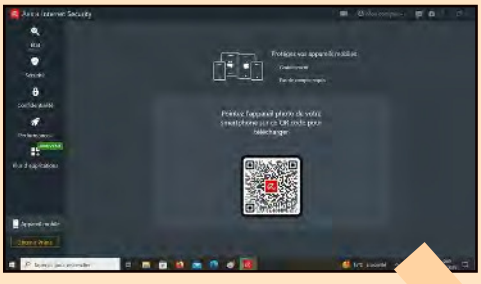


3 Une fois opérationnel, Avira suggérera un premier passage au scan de votre ordinateur pour établir un diagnostic (problèmes de confidentialité, de performances, présence de virus, applications obsolètes).

4 Ce premier bilan révélera probablement quelques bugs, pas forcément graves. Notre ordinateur de tests était exempt de virus, mais comportait, par exemple, des applis obsolètes et des cookies curieux. Vous pourrez corriger en cliquant sur « Résoudre les problèmes », une opération qui a exigé une vingtaine de minutes environ.



5 L'interface d'utilisation d'Avira Internet Security est très simple. Organisée par onglets, elle permet d'accéder en un clic aux options de protection (anti-rançongiciel, pare-feu, etc.), de confidentialité (protection du navigateur, VPN, destructeur de fichiers) et de performances (libérer de l'espace, optimiser la batterie, etc.).



6 À gauche, en bas de la colonne du menu, vous trouverez un onglet « Application mobile ». Pointez simplement l'appareil photo de votre tablette ou de votre smartphone (Android, iOS) afin de scanner le QR code. Il vous dirigera vers le téléchargement de l'appli Avira pour protéger gratuitement vos appareils mobiles.

Antivirus en ligne
UNE OPTION À ÉTUDIER

Les antivirus que l'on peut trouver en ligne sont souvent gratuits et ne nécessitent pas d'installation sur votre ordinateur. S'ils sont faciles à utiliser et performants, ils présentent quelques inconvénients. On fait le point.

Les antivirus en ligne sont des logiciels de sécurité qui vont scanner les fichiers et les programmes présents sur votre ordinateur ou sur votre appareil mobile (tablette, téléphone…), afin de détecter et de supprimer d'éventuels virus. Ils fonctionnent de différentes manières, mais la plupart d'entre eux mettent en œuvre des combinaisons de techniques pour repérer les attaques. Parmi celles-ci, les plus courantes incluent l'analyse heuristique, qui consiste à examiner le comportement des fichiers afin de détecter les menaces potentielles, et l'étude de signatures, autrement dit la comparaison des éléments avec une base de données répertoriant les signatures de *malwares* connus.

Certains antivirus en ligne recourent également à des analyses comportementales ou de réputation, entre autres. Les outils comme VirusTotal, Hybrid Analysis, Jotti's Malware Scan ou encore MetaDefender Cloud sont reconnus pour bien déceler les menaces du type adresses web malveillantes ou fichiers piégés, en passant tout au peigne fin. Par exemple, VirusTotal propose un service gratuit qui exploite plus de 60 antivirus. Il suffit que l'internaute présente un lien ou télécharge un dossier suspect directement sur le site, et un rapport est généré en quelques dizaines de secondes (selon la taille du fichier).

Il faut toutefois être conscient qu'envoyer et soumettre ainsi des documents – de type Word, Excel ou autre – qui sont potentiellement sensibles à une analyse, c'est courir le risque de compromettre leur confidentialité… Enfin, il est à noter que certains cybercriminels testent leurs créations sur VirusTotal avant de les lancer !

ENVIRON 500 000 NOUVEAUX MALWARES PAR JOUR FIN 2024

Selon l'éditeur d'antivirus français AxBx, par rapport à 2021, un internaute avait, en février 2023, six fois plus de risques d'être exposé à un *malware* de type voleur de mot de passe, et quatre fois plus de risques de rencontrer un *ransomware*. La tendance ne faiblit pas : l'AV-Test Institute enregistre désormais près de 450 000 nouveaux programmes ou applications indésirables chaque jour, soit plus de 1,2 milliard d'échantillons distincts recensés fin 2024. Statista et AV-Test indiquent une moyenne plus élevée, autour de 560 000 nouveaux logiciels malveillants quotidiens. Et les malfaiteurs diversifient leurs cibles : Kaspersky relève une hausse de 29 % des attaques Android au premier semestre 2025, avec une explosion des *trojans* (chevaux de Troie) bancaires mobiles, multipliés par quatre en un an. Du côté du Multi-State Information Sharing and Analysis Center (MS-ISAC), les *malwares* de type *downloaders* (téléchargements furtifs) dominent : le SocGholish représente ainsi près de 48 % des détections observées au premier trimestre 2025.

Une solution efficace… mais qui ne garantit pas la confidentialité.

De fait, si cet outil spécialisé ne détecte rien, cela signifie que leurs programmes malveillants seront radicalement efficaces…

De vrais avantages

Face aux antivirus traditionnels, parfois lourds, qu'il faut charger sur un ordinateur, ceux en ligne affichent divers atouts. Premièrement, ils sont plus faciles à utiliser, puisqu'ils ne nécessitent ni installation ni mise à jour manuelle. Deuxièmement, ils sont en général gratuits, ce qui les rend accessibles à tous. Enfin, ces outils se révèlent souvent plus performants que les classiques, car ils sont actualisés en permanence pour lutter contre les nouvelles menaces dès leur apparition. Cela constitue un véritable avantage, car de nombreux internautes pensent qu'une fois qu'ils ont un antivirus sur leur PC, ils sont protégés et n'ont plus rien à faire… Or, s'ils oublient d'effectuer les indispensables mises à jour des signatures de virus et autres codes malveillants, leur logiciel de sécurité ne servira plus à grand-chose assez vite. *suite p. 110* >>

M. H. NIZAMUDEEN/ISTOCK

VIRUS LÉGENDAIRES

> **Brain** (le « cerveau ») est le premier virus connu. Il a été créé en 1986 au Pakistan par les frères Basit et Amjad Farooq Alvi. Ayant une entreprise informatique à Lahore, ils voulaient suivre le nombre de disquettes qu'ils avaient vendues. Brain infectait ces dernières et se propageait par les ordinateurs personnels. Toutefois, il n'avait pas pour objectif de causer des dommages ou de voler des données, il contenait juste un message proposant de contacter les informaticiens.

> **Happy99,** le bienheureux, a été écrit par un programmeur néerlandais du nom de Jan de Wit pour fêter 1999. Bien que ce virus ne soit pas considéré comme particulièrement dangereux, il a été l'un des premiers à se propager largement sur Internet, par courrier électronique.

> **Stuxnet** est considéré comme l'un des logiciels les plus agressifs mis au point. Il a été utilisé pour attaquer le programme nucléaire iranien en 2010. On pense qu'il a été conçu par une équipe de pirates travaillant pour des pays occidentaux, dont les États-Unis et Israël.

> **Zeus et SpyEye** sont des *malwares* bancaires ayant servi à voler des centaines de millions d'euros dans les années 2010. Ils ont été créés par les criminels russes Evgeniy Bogachev et Aleksandr Andreevich Panin. Le premier vit caché en Russie, le second est en prison aux États-Unis depuis 2013.

> **LockBit, Royal, DeadBolt, Bozon, Qakbot…** tels sont les noms des codes malveillants occasionnant, à l'heure actuelle, des milliards de pertes de données.

Interview

CLARISSE Pirate de cartes bancaires à 16 ans

« ON SE SENTAIT LES ROIS »

Le pirate n'est pas toujours, comme on l'imagine, une silhouette mystérieuse tapie derrière un écran à l'autre bout du monde… Parfois, il est assis sur votre canapé. Cette interview en est la preuve. Insouciance, inconscience et appât du gain peuvent transformer une adolescente ordinaire en cybercriminelle. Cette histoire rappelle à quel point la vigilance débute à la maison.

Q C Comment avez-vous commencé le piratage de cartes bancaires (*carding*) ?

Clarisse L'idée est venue par deux amis. Un jour, ils sont arrivés avec de nouveaux vêtements, de nouvelles chaussures, un nouveau téléphone. Ils payaient le McDo à tout le monde. À 16 ans, en étant au lycée… On s'est demandé d'où venait tout cet argent. Papa, maman ? Non. En fait, c'était un business. J'ai voulu tester aussi, peut-être gagner 50 € par jour. Ils m'ont montré un site, Card House. C'était l'Alibaba des cartes bancaires: des Visa, des Mastercard, pour 5 ou 10 €. Mon pote connaissait même les modérateurs, ceux qui géraient le site. Quand une carte ne fonctionnait pas, on était remboursé. J'en ai acheté une, ça n'a pas marché, hop remboursement, puis une autre…

Q C Comment les achetiez-vous ?

C. Avec ma carte bancaire, via un portefeuille crypto (BTC ou Ethereum). Avec seulement 50 €, j'obtenais de 5 à 10 cartes.

Q C Et vous faisiez quoi avec ?

C. Rien de fou: je me payais des restaurants, des chaussures à la mode, des vêtements, parfois pour 100 à 200 € d'achats. En tout, ça m'a rapporté environ 3 000 €, pour à peine 300 à 400 € de dépenses en cartes piratées.

Q C Vous ne pensiez pas aux victimes derrière ces cartes ?

C. Non… à 16 ans, on voulait juste suivre la mode. Avoir des Nike, un iPhone. On ne pensait pas du tout à Madame Dupont derrière son compte.

Q C Malgré toutes ces dépenses, vos parents ne se doutaient de rien ?

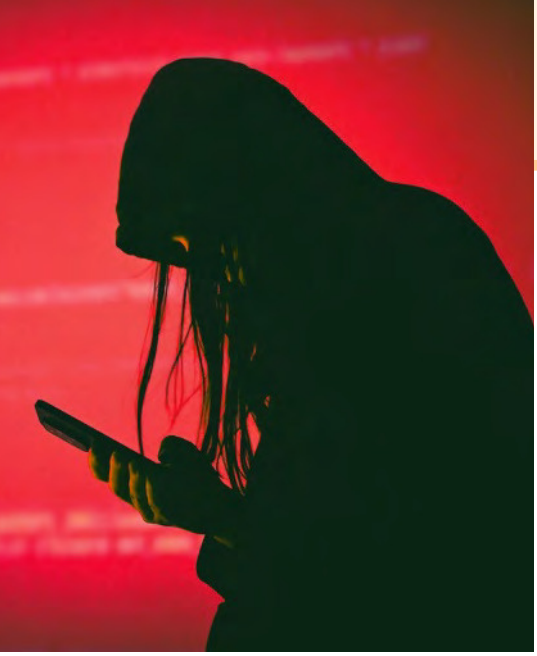
C. Pas vraiment. J'achetais des parfums ou des petites choses que mes parents n'imaginaient pas chers. Ils ne vérifiaient pas.

Q C Et vos amis ?

C. On se sentait les rois. Parfois, j'offrais des parfums à des copines, comme si j'étais une grande. En vrai, c'était grisant de pouvoir acheter ce que je voulais, quand je le voulais.

Q C Votre entourage était donc plongé dans ce milieu ?

C. Oui. Mon pote, lui, en a fait un véritable business. Il a acheté une machine à laver pour sa mère, des consoles de jeux, etc. Il a carrément arrêté les cours, et sa mère était complice… Mais il a fini par être recherché par Interpol. Il vit aujourd'hui caché, en Airbnb qu'il paie en liquide. Il n'a plus d'avenir… [À noter que notre témoin a appelé son ami pendant l'interview afin que nous lui parlions. Réponse: «*Il ne peut pas vous répondre pour le moment, il a quelques problèmes.*»].



Y. TABA/ISTOCK

Aviez-vous aussi des pratiques telles que les « Allos » (ces appels téléphoniques servant à extorquer des codes) ?

C. Au lycée, certains faisaient ça pour 50 €. Des copines appelaient, entre deux cours, pour récupérer des codes permettant ensuite de voler l'argent. Moi, non. Mais j'ai servi de mule en allant chercher des colis achetés frauduleusement.

Avec du recul, comment voyez-vous cette période ?

C. À 16 ans, on ne pense qu'à l'argent facile. Aujourd'hui, à 22 ans, je comprends que ce sont de vraies victimes, parfois des familles qui perdent leurs économies. Je n'y pensais pas à l'époque.

N'avez-vous jamais eu de problème avec la justice ?

C. Une fois, si. Un pote avait fait une commande à mon vrai nom. J'ai reçu une lettre de la boutique: impayé de 300 €. J'ai dû aller porter plainte contre X et dire que je n'y étais pour rien !

Vous craignez des poursuites ?

C. J'ai longtemps été en panique. À présent, si ça tombe, j'assumerai. Et je veux surtout alerter: c'est une spirale dangereuse. On croit que c'est cool, mais ça détruit des vies, y compris la vôtre. ■

ADOLESCENTS BASCULER DANS LA CYBERCRIMINALITÉ ARRIVE VITE

En septembre 2025, la National Crime Agency (NCA), qui lutte contre le crime organisé au Royaume-Uni, avertit : la frontière entre l'expérimentation technique et la cybercriminalité s'estompe chez les jeunes. Son programme Cyber Choices, conçu pour réorienter ces profils vers des utilisations légales, a même identifié des cas dès l'âge de 7 ans. Selon la NCA, un enfant sur cinq âgé de 10 à 16 ans s'est déjà livré à des activités illicites en ligne dans le pays. L'Information Commissioner's Office (ICO), l'autorité britannique chargée de la protection des données, note que 5 % des ados de 14 ans déclarent avoir piraté un système informatique. La France ne fait pas mieux face à cette exposition précoce. Une enquête menée dans des collèges et lycées hexagonaux, en septembre 2025, par le site Zataz illustre le phénomène.

Exposition massive

Tous les élèves interrogés (47 tirés au sort sur 360) s'étaient servis d'Internet juste après leur réveil. Plus d'un sur cinq (21,3 %) a déjà été victime ou témoin d'un piratage, visant principalement des comptes de réseaux sociaux. La même proportion sait les mots de passe de ses parents, et 6,4 %, ceux de leurs camarades de classe. L'usage de l'intelligence artificielle est évident : 93,6 % citent ChatGPT, certains mentionnent aussi DeepSeek ou Gemini. La présence sur TikTok, Instagram et consorts est considérable : 55,3 % gèrent de un à trois comptes, 40 %, plus de trois, et seuls 6,4 % ne sont inscrits nulle part. Le recours à des pratiques risquées est tangible : un collégien de 13 ans connaissait déjà un *lookup*, un agrégateur pirate exploitant des fuites de données en temps réel. En outre, 34 % des jeunes ont admis avoir employé un mot de passe qui n'était pas le leur, 40,4 % ont téléchargé un logiciel de triche (souvent vecteur de programmes malveillants), 6,4 % ont testé un enregistreur de frappe et 4,3 %, un voleur d'informations. Seuls 55,3 % des sondés ont affirmé n'avoir jamais touché à des logiciels piratés. Ces chiffres confirment que l'exposition au cyberespace est incontournable, et que le passage à des pratiques criminelles se produit parfois très tôt, même involontairement.

Sources : ICO et Zataz.

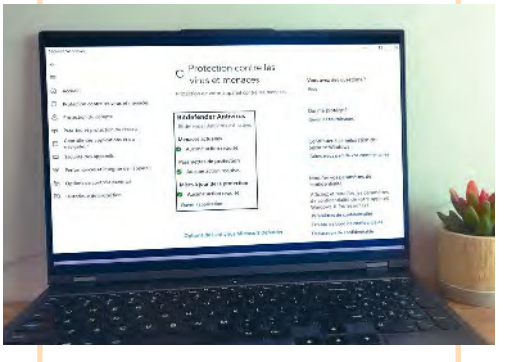
Attention, les antivirus gratuits ne lancent des analyses que lorsque vous le leur demandez…

… Et de gros inconvénients

Les antivirus en ligne présentent néanmoins des désavantages. D'abord, ils nécessitent une connexion Internet à haut débit afin de pouvoir fonctionner, ce qui constitue un frein réel si l'on n'en dispose pas. Surtout, ils sont susceptibles de poser des problèmes de confidentialité (lire plus haut), car ils doivent accéder à vos fichiers pour les analyser. Un exemple de mésaventure que cela risque d'entraîner ? En 2017, un consultant travaillant pour la NSA, l'Agence de sécurité nationale américaine, a perdu le contrôle de fichiers ultra-confidentiels appartenant à cet organisme de services secrets après que son logiciel a repéré des codes malveillants. Par la suite, l'homme a été accusé de piratage, et l'éditeur de l'antivirus, d'espionnage… Enfin, cet outil en ligne analyse le contenu de votre appareil seulement quand vous lancez l'opération : la protection est donc ponctuelle, alors qu'un antivirus installé sur votre ordinateur et mis à jour régulièrement fonctionne en arrière-plan. Il sera ainsi en mesure de détecter en permanence les nouvelles menaces afin de les contrer. ■

PROTÉGEZ VOTRE PC AVEC MICROSOFT DEFENDER

Lors d'une attaque par rançongiciel, par exemple, vos fichiers les plus importants peuvent être chiffrés et pris en otage. Dans Windows 10 et 11, l'outil Microsoft Defender vous permet de les protéger grâce à l'accès contrôlé. Le principe ? Seules les applications connues et approuvées figurant sur une liste ont la possibilité d'accéder à vos dossiers. Celles qui ne sont pas autorisées sont bloquées. Et, lorsqu'une appli tente de modifier un fichier dans un dossier protégé, Microsoft Defender vous envoie une notification. Le logiciel gère la liste des applications fiables, mais vous êtes aussi en mesure d'en ajouter manuellement. Les dossiers système courants, ainsi que tous ceux que vous aurez choisis, seront sécurisés de la sorte. Pour activer



cette fonctionnalité, rendez-vous dans Microsoft Defender, sélectionnez « Démarrer », puis « Paramètres », « Mise à jour et sécurité », « Sécurité Windows » et « Protection contre les virus et menaces ». Il ne vous reste plus qu'à gérer les paramètres.

TIERO ; PITER2121/ADOBE STOCK

COMPRENDRE LES MOTS

Pas toujours facile de saisir le vocabulaire du numérique ! Voici donc un petit dictionnaire qui vous y aidera.

Adresse électronique (e-mail) jetable Valable seulement quelques heures ou quelques jours, elle vous évite de donner votre véritable adresse.

Adresse IP Numéro unique identifiant votre appareil (ordinateur, smartphone…) sur Internet.

AI Act Règlement européen entré en vigueur en août 2024 contraignant ou interdisant certains usages de l'intelligence artificielle jugés dangereux, comme la reconnaissance faciale de masse ou le *scoring* social.

Alias e-mail Adresse secondaire liée à la principale, créée pour séparer ses usages (professionnels, de loisirs, marchands…).

Amende RGPD Pénalité financière imposée à une organisation publique ou privée pour non-respect des règles de protection des données (jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial).

AMF L'Autorité des marchés financiers est un organisme public français qui contrôle les placements financiers et protège les investisseurs.

Archive.org Aussi appelé *The Wayback Machine,* ce site conserve des copies d'anciennes pages web.

Arnaque Tromperie visant à soutirer de l'argent ou des informations.

Authentification à deux facteurs (2FA/MFA) Système de sécurité demandant une seconde preuve d'identité pour autoriser un accès (par exemple, code SMS + mot de passe).

BIC Code identifiant la banque lors des virements internationaux.

BleachBit Outil de nettoyage effaçant les fichiers inutiles et supprimant les traces numériques de façon sécurisée.

Bruteforce attack L'«attaque par force brute» est une méthode de piratage qui teste automatiquement des milliers de combinaisons pour trouver un mot de passe.

Cheval de Troie («troyen» ou *trojan horse*) Programme malveillant caché dans une application ou un fichier qui cherche à ouvrir la porte aux pirates.

Chiffrement Technique de transformation des données en code secret illisible sans clé spéciale, ce qui les protège en cas de vol ou d'interception.

Clearview AI et PimEyes Outils de recherche identifiant des personnes sur Internet grâce à une photo.

Cloud Stockage de données sur Internet (et non uniquement sur son appareil).

L. CHERNETSKA/ISTOCK

Cloud Act Loi permettant aux autorités des États-Unis d'accéder à des données stockées par des entreprises américaines, même installées en Europe.

Cnil La Commission nationale de l'informatique et des libertés est l'autorité française qui protège nos données personnelles et veille à leur bon usage.

Consentement Accord donné librement pour l'utilisation de ses données personnelles.

Cookies Fichiers créés par les sites web et stockés sur les ordinateurs des internautes pour retenir leurs préférences ou suivre leur navigation.

Coppa La Children's Online Privacy Protection Act est une loi américaine protégeant la vie privée en ligne des enfants.

Credential stuffing Piratage consistant à tester automatiquement des mots de passe volés sur d'autres comptes.

Cryptographie Science des messages secrets regroupant le chiffrement, la cryptanalyse (casser un code) et la stéganographie (cacher un message dans un support – une image, par exemple).

Cryptomonnaie Monnaie numérique (comme le bitcoin, l'Ethereum, le Monero, etc.).

Cyberattaque Assaut informatique mené via Internet pour voler, bloquer ou détruire des données.

Cybermalveillance.gouv.fr Plateforme officielle française d'aide aux victimes d'attaques et d'arnaques en ligne.

DBAN Le Darik's Boot and Nuke est un programme qui efface complètement un disque dur en écrasant toutes les données, les rendant irrécupérables.

Deepfake Vidéo ou image truquée générée par intelligence artificielle pour faire croire à une fausse réalité.

Directive européenne Texte adopté par l'Union européenne qui doit être appliqué et transposé dans les lois nationales.

DNSLytics Outil donnant des informations techniques sur un site (nom de domaine, hébergeur, localisation…).

Dork (ou Google *dorking*) Commande spéciale utilisée dans un moteur de recherche pour trouver des données précises.

DPF EU-US Le Data Privacy Framework est un accord entre l'Europe et les États-Unis sur la protection des données transférées entre les deux continents.

DPO Le délégué à la protection des données est la personne chargée de protéger les données personnelles dans une entreprise.

Droit à l'oubli Droit de tout internaute de demander la suppression d'informations personnelles sur Internet.

Fake news Fausse information diffusée en ligne pour tromper ou manipuler.

Firewall («pare-feu») Outil bloquant les connexions internet suspectes afin de protéger un appareil.

FTC La Federal Trade Commission est l'autorité américaine qui protège les consommateurs et sanctionne les abus.

Gestionnaire de mots de passe Logiciel créant et gardant en mémoire des mots de passe complexes à votre place.

HTTPS Version sécurisée d'un site web (indiquée par un cadenas dans la barre d'adresse).

Hunter.io Site permettant de vérifier si une adresse e-mail est réellement utilisée par une entreprise.

Iban Numéro international permettant d'identifier votre compte bancaire.

Identité numérique Ensemble des informations qui vous représentent en ligne (nom, photos, e-mails, comptes…).

Imei Numéro unique d'identification d'un téléphone portable. Pour le connaître, tapez *#06 sur votre clavier.

IMSI-catcher Boîtier capable d'intercepter les communications téléphoniques mobiles. Il est utilisé par les services de renseignement… mais aussi par des pirates.

Ingénierie sociale Manipulation psychologique destinée à vous pousser à révéler des informations ou à exécuter une action.

Intelligence artificielle (IA) Tout outil utilisé par une machine capable de reproduire des comportements liés aux humains.

KeePassXC Gestionnaire de mots de passe stockant tous vos identifiants dans un coffre-fort chiffré, accessible avec un seul mot de passe maître.

Likee Réseau social vidéo installé à Singapour, concurrent de TikTok, critiqué pour son accès facile à des contenus inappropriés.

Logs Historiques enregistrés automatiquement par un ordinateur ou une appli: connexions, erreurs, périphériques utilisés, etc.

Machine learning L'«apprentissage automatique» est une technique d'intelligence artificielle qui apprend à partir de grandes quantités de données, par l'intermédiaire de modèles mathématiques.

Majorité numérique Âge minimal fixé par la loi pour utiliser un réseau social sans autorisation parentale (15 ans, en France).

Malware Programme malveillant conçu pour infecter un ordinateur ou un téléphone.

Métadonnées Informations cachées dans un fichier (date, auteur, appareil utilisé…).

Mot de passe Code secret (lettres, chiffres, symboles) qui protège l'accès à vos comptes.

NFC La technologie *Near Field Communication* permet d'échanger des données sans contact (comme le paiement sans contact).

NIS 2 Nouvelle directive européenne renforçant la sécurité des réseaux et des systèmes informatiques (elle traite notamment des secteurs critiques, des sanctions et des critères de transparence).

.onion Extension de site internet accessible uniquement via le réseau TOR, utilisé pour l'anonymat.

Osint L'*Open Source Intelligence* est une méthode de collecte d'informations à partir de sources publiques (sites, réseaux sociaux, images satellites).

Passkey Nouvelle méthode de connexion sans mot de passe, qui utilise votre empreinte, votre visage ou un code PIN.

PCLOB Le Privacy and Civil Liberties Oversight Board est une instance américaine qui surveille la protection des libertés face aux programmes de surveillance.

Phishing (hameçonnage) Arnaque via des e-mails ou des SMS imitant une banque, un opérateur ou un service officiel pour voler vos identifiants.

Portabilité des données Droit de récupérer ses informations personnelles et de les transférer ailleurs.

Proton Mail Service d'e-mails sécurisé installé en Suisse. Les messages sont chiffrés et les données, protégées par des lois strictes sur la vie privée.

Qubes OS Système d'exploitation conçu pour la sécurité. Il compartimente chaque application dans un espace isolé, limitant les risques d'attaque.

RAM (mémoire vive) Mémoire temporaire de l'ordinateur, qui enregistre les données utilisées pendant son fonctionnement. Tout s'efface quand on éteint la machine.

Ransomware Un «rançongiciel» est un programme informatique malveillant qui bloque vos fichiers et réclame une rançon pour les libérer.

RGPD Le Règlement général sur la protection des données est une loi européenne encadrant la récolte, le traitement et l'usage des informations personnelles (droit à l'oubli, obligation de consentement…).

RIB Le relevé d'identité bancaire est un document contenant vos coordonnées bancaires (Iban, BIC).

Safe zone Espace virtuel sécurisé dans un jeu vidéo, où les jeunes peuvent poser des questions ou demander de l'aide.

Scoring social Système d'évaluation basé sur vos comportements en ligne (achats, recherches, paiements…), pouvant influencer vos droits. Interdit en Europe désormais.

Signal Application de messagerie chiffrée. Les messages et les appels ne peuvent être lus ou écoutés que par l'expéditeur et le destinataire.

SIM swapping Technique de piratage consistant à détourner votre numéro de téléphone vers une nouvelle carte SIM contrôlée par un pirate.

Spyware Ce «logiciel espion», installé à votre insu sur votre appareil (smartphone, tablette, ordinateur), surveille vos activités et vole vos données.

Tails Système d'exploitation portable qui démarre depuis une clé USB. Il ne laisse aucune trace sur l'ordinateur utilisé et intègre par défaut des outils de sécurité.

Tchat vocal Discussion audio en direct sur une plateforme ou un jeu en ligne.

TOR Logiciel permettant de naviguer anonymement sur Internet en masquant son adresse IP.

URL Adresse web.

VeraCrypt Logiciel gratuit permettant de chiffrer des fichiers, dossiers ou disques entiers afin de les rendre illisibles sans mot de passe.

Vishing Phishing par appel téléphonique.

VPN Le *Virtual Private Network,* ou «réseau privé virtuel», est un service cachant votre adresse IP et chiffrant vos connexions internet.

Vulnérabilité Faiblesse dans un logiciel ou un système qu'un pirate peut exploiter.

Watermarking Ce filigrane numérique est une marque invisible ajoutée sur un contenu en ligne pour prouver son authenticité.

Zero-day («jour zéro») Faille informatique toute neuve, encore inconnue des fabricants, exploitée par les pirates.

HUILE D'OLIVE

Apprenez à la choisir

Comment acheter une bonne huile d'olive ? Sur les étiquettes, les mentions fleurissent. Difficile de distinguer informations réelles sur la qualité du produit et allégations marketing… Choisir une huile d'olive, par ailleurs, c'est également une question de goût, de budget et d'usage. Voici quelques repères pour vous guider.

*Par **Marie-Noëlle Delaby** et **Elsa Casalegno***

EYEEM/ISTOCK

Connaître la proven

Trouver une bonne huile et, surtout, savoir d'où elle vient n'est pas forcément évident, tant l'étiquetage peut être vague. Il existe néanmoins des labels auxquels se raccrocher.

Préciser, sur l'étiquette, la provenance des huiles vendues dans l'Union européenne (UE) est obligatoire. On affiche à la fois l'origine des olives et le lieu de production. Pour les références qui ne bénéficient pas d'une appellation d'origine protégée (AOP) ou d'une indication géographique protégée (IGP), cela consiste en une simple mention à un pays ou à l'UE. Le consommateur n'est alors pas forcément mieux informé, car la plupart des produits commercialisés comportent des mélanges d'huiles de divers États (Espagne, Grèce, Italie, Tunisie…), signalés en général ainsi: «huiles d'olive de l'Union européenne», ou encore «assemblage d'huiles d'olive originaires de l'UE et non originaires de l'UE». Autant dire le monde entier!

Enfin, l'indication d'un pays d'origine unique ne garantit pas un meilleur produit, notamment lorsqu'il s'agit de très gros producteurs d'huile d'olive comme l'Espagne (qui représente à elle seule environ 50% du marché mondial), l'Italie ou la Tunisie, où tous les niveaux de qualité coexistent.

Privilégier les labels de qualité

Toutefois, si l'on cherche une huile typée, mieux vaut s'orienter vers des articles sous signe de qualité AOP ou IGP, qui marquent le lien avec le terroir – entendu au sens large (sol, climat, savoir-faire). On compte une centaine d'appellations d'origine en Europe, dont 42 en Italie, 26 en Espagne et 9 en France (lire l'encadré ci-contre). Le nom géographique associé à un signe lui est réservé (une huile qui n'est pas sous AOP Huile d'olive de Corse ne peut pas mentionner «Corse», par exemple).

Vérifier sa présence permet d'éviter les fausses huiles «de terroir» parfois proposées sur les marchés provençaux, les foires ou les stands de bords de route. Et quand l'origine France n'est pas indiquée, c'est qu'il s'agit de produits d'assemblage issus de l'UE… vendus moitié moins cher en grandes surfaces.

Du bassin méditerranéen, mais pas que

Une large majorité, à savoir 97% de l'huile d'olive, provient du bassin méditerranéen, où se trouvent les pays traditionnellement producteurs. À elle seule, l'UE – principalement l'Espagne, la Grèce et l'Italie – en fournit 70%. Cependant, la culture de l'huile d'olive s'est mondialisée, et des oliviers poussent désormais aux États-Unis, dans une grande partie de l'Amérique du Sud et même en Australie et en Nouvelle-Zélande. Par ailleurs, à cause du réchauffement climatique, les volumes récoltés peuvent varier de façon importante d'une année à l'autre, et entraîner des baisses de qualité globale de l'huile d'olive. ■

Les 9 AOP françaises

- AOP huile d'olive **d'Aix-en-Provence**
- AOP huile d'olive **de Corse**
- AOP huile d'olive **de Haute-Provence**
- AOP huile d'olive **du Languedoc**
- AOP huile d'olive **de Nice**
- AOP huile d'olive **de Nîmes**
- AOP huile d'olive **de Nyons**
- AOP huile d'olive **de Provence**
- AOP huile d'olive **de la vallée des Baux-de-Provence**

ance


GAISA/ADOBE STOCK

LE MARCHÉ DES HUILES D'OLIVE EN FRANCE

Conséquence de l'engouement pour le régime crétois, notre consommation d'huile d'olive est stable depuis les années 2000, après avoir triplé en 15 ans : environ 2 l par habitant/an. C'est la quatrième huile la plus consommée en France derrière celles de tournesol, de colza et de palme (cette dernière étant présente dans les aliments transformés), et la deuxième la plus vendue en grande distribution après celle de tournesol. La production nationale, modeste (0,16 % de la production mondiale), est très inférieure à nos besoins. Ces 20 dernières années, elle n'a représenté que 4 % de la consommation hexagonale, largement dominée par l'Espagne (leader en conventionnel), l'Italie et la Tunisie (leader en bio). L'huile française se positionne essentiellement dans le haut de gamme, avec 30 % des volumes sous AOP, et des prix autour de 25 € le litre. Les huiles d'olive « vierge extra » sont les préférées des Français (80 % de la consommation) et, parmi elles, les références bios progressent (soit environ 20 % du marché). Les leaders dans cette catégorie (hors bio) sont Puget, Carapelli, Terra Delyssa et Tramier. Mais ce sont les marques de distributeurs (MDD) qui dominent les ventes en grandes surfaces, avec 39 % de parts de marché.

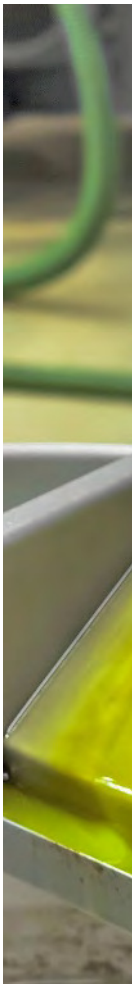
Les principaux pays producteurs en 2024-2025

	PRODUCTION EN TONNES (1)	ÉVOLUTION (2)
ESPAGNE	1289900	+51 %
TURQUIE	450000	+109 %
TUNISIE	340000	+5 %
GRÈCE	250000	+43 %
ITALIE	224000	-32 %
PORTUGAL	195000	+21 %
SYRIE	105000	+31 %
MAROC	90000	-15 %
PRODUCTION MONDIALE	3197000	-0,3 %

(1) Prévisionnelle. (2) Par rapport à 2023-2024. Source : Conseil oléicole international.

Bien différencier les

Les dénominations des huiles d'olive sont strictement réglementées, sous l'égide du Conseil oléicole international. On fait le point.



J. TOMIC/ADOBE STOCK

VIERGE EXTRA
Le haut du panier

On obtient cette huile de qualité supérieure par pression à froid (lire l'encadré «Comment fait-on de l'huile ?» p. 119), sans chauffage. Elle répond à des critères très stricts, conjuguant un test de dégustation par des experts agréés par le Conseil oléicole international (COI, une organisation intergouvernementale) et des analyses physico-chimiques irréprochables (une certaine teneur en acide oléique, par exemple). Le moindre défaut lui vaut de perdre le qualificatif «extra» et de se contenter du «vierge».

VIERGE
Pure, mais pas absolument irréprochable

Les procédés d'extraction de l'huile «vierge» sont uniquement mécaniques ou physiques, sans traitement chimique, et avec un éventuel chauffage doux. Elle est pure (non mélangée à d'autres huiles), non raffinée et peut être consommée en l'état. Mais elle présente des défauts mineurs qui ne permettent pas de la classer en «vierge extra».

LAMPANTE
Impropre à la consommation

Ses défauts trop nombreux (forte acidité, goût désagréable) la rendent impropre à la consommation. Elle ne peut pas être vendue, et est destinée aux industries du raffinage ou à des usages techniques. Pour être employée en alimentaire, elle doit être raffinée puis mélangée à de l'huile vierge.

RAFFINÉE
Processus industriel et mélange

Cette huile est obtenue par raffinage d'huiles d'olive vierges, via un processus industriel spécifique (solvants, centrifugation, filtration, lavage et séchage à haute température). La substance obtenue est ensuite mélangée avec de l'huile d'olive «vierge» ou «vierge extra» pour être vendue sous la dénomination «huile d'olive».

HUILE D'OLIVE
Le fruit d'un coupage

Il s'agit d'un produit constitué par le coupage d'huile d'olive raffinée avec des huiles d'olive vierges propres à la consommation en l'état.

HUILE DE GRIGNONS D'OLIVE
Rien ne se perd !

Les grignons d'olive sont les résidus solides (peau, pulpe, fragments de noyaux) issus du processus d'extraction de l'huile d'olive. On les traite en recourant à des solvants ou à d'autres procédés physiques pour en tirer de l'huile. Celle-ci se divise en trois catégories: l'huile de grignons d'olive brute, non comestible et destinée au raffinage (elle sert notamment de base dans la fabrication de savons); l'huile de grignons d'olive raffinée, neutre en goût et non commercialisée directement pour l'alimentation; et enfin l'huile de grignons d'olive, obtenue par coupage d'huile de grignons d'olive raffinée et d'huiles d'olive vierges, qui est surtout dédiée à la cuisson ou à la friture. ■

catégories

On extrait l'huile à froid (moins de 27 °C) pour préserver ses qualités, par pressage ou centrifugation.

COMMENT EST-ELLE FABRIQUÉE ?

Malgré les innovations techniques, la production de l'huile d'olive obéit aux mêmes principes depuis l'Antiquité. Après la récolte, les olives, noyaux inclus, sont écrasées dans une meule ou un broyeur pour former une pâte, laquelle est ensuite malaxée. L'étape suivante est celle de l'extraction de l'huile, à froid (c'est-à-dire à une température inférieure à 27 °C) afin de préserver ses qualités. Il existe deux techniques principales pour cela :

> **la pression à froid** (méthode traditionnelle), où l'huile est extraite par pression de la pâte au moyen d'une presse. À noter : la mention « première pression à froid » sur l'étiquette n'est plus autorisée (lire l'encadré ci-dessous « Gare aux pièges du marketing ! ») ;

> **l'extraction à froid** (processus moderne), durant laquelle la pâte tourne à grande vitesse dans une centrifugeuse, ce qui entraîne la séparation de l'eau, de la pâte et de l'huile en raison de leurs densités différentes.

GARE AUX PIÈGES DU MARKETING !

Attention : la mention « première pression à froid » sur une huile d'olive n'est plus autorisée. Non prévue par la réglementation, elle signifie en effet que l'huile est obtenue par un chauffage à moins de 27 °C, qui n'altère pas ses qualités. Or, c'est aujourd'hui un prérequis pour toutes les huiles d'olive « vierge extra », cela la rend donc obsolète. Autrefois, une deuxième pression avec de l'eau chaude était nécessaire pour extraire la totalité de l'huile. Grâce aux progrès techniques, elle n'est plus utile, et cette précision est devenue un argument de vente illicite. De même, l'allégation « récolte manuelle » n'est pas prévue par la réglementation.

Identifier toutes les

Comme le vin, l'huile d'olive est un produit vivant et complexe, offrant divers arômes et saveurs qui reflètent la variété du fruit, le terroir, le moment de la récolte et le savoir-faire du producteur.

Savoir déguster une huile d'olive n'est pas inné. Cela s'apprend, afin d'être en mesure d'apprécier pleinement toute la variété des produits. En la matière, votre palais sera toujours meilleur guide que votre nez… En effet, une huile au parfum puissant n'est pas forcément riche en goût, et inversement. Il existe d'ailleurs trois familles de saveur pour les huiles d'olive, classées selon leur fruité: goût intense (fruité vert), subtil (fruité mûr) et maturé, dit aussi à l'ancienne (fruité noir). Mais qu'est-ce que le «fruité»? Ce terme renvoie à l'ensemble des sensations olfactives et gustatives que procure une huile. Il dépend grandement du moment de la récolte… On vous explique tout.

COMMENT LA GOÛTER ?

L'huile d'olive se déguste d'une certaine manière afin d'apprécier sa complexité aromatique et gustative.

- **Versez-en** un peu dans un petit verre.
- **Chauffez-la doucement** en plaçant le verre dans le creux d'une main et en le couvrant de l'autre. Faites tourner l'huile.
- **Retirez la main sur le verre et sentez les arômes.** Recommencez plusieurs fois pour percevoir toutes les nuances.
- **Prenez une petite gorgée d'huile.** Faites-la bien tourner dans votre bouche, puis aspirez un peu d'air entre les dents.
- **Identifiez le type de fruité,** l'amertume ressentie et le piquant. Soyez aussi attentif à la texture et à la persistance des saveurs.

R. SCALIA/ADOBE STOCK

FRUITÉ VERT
Un goût intense

Le fruité vert caractérise les huiles issues d'olives cueillies quelques jours avant leur pleine maturité, quand leur couleur est «tournante» ou légèrement «purpurine», c'est-à-dire qu'elle passe du vert au mauve. Ce sont souvent les plus qualitatives, car les plus aromatiques et les plus riches en polyphénols. Au nez et en bouche, les notes herbacées dominent. On y décèle des arômes d'artichaut, de poivron et de fruits verts. Ces huiles peuvent présenter de l'ardence (une sensation de piquant similaire à celle procurée par les épices) ou de l'amertume, dues à la fraîcheur des olives au moment de la trituration (opération consistant à broyer les olives avant d'en extraire l'huile). Si les italiennes sont particulièrement réputées pour leur fruité vert, on en trouve également en France, en Andalousie ou dans le nord de la Catalogne.

FRUITÉ MÛR
Une saveur subtile

Le fruité mûr s'obtient avec des olives ramassées à maturité et noires. L'huile a alors des saveurs plus douces (peu ardentes et peu amères) et rondes en bouche, avec des arômes d'amande, de fruits rouges ou jaunes, de tilleul ou de fleurs. Les huiles espagnoles et tunisiennes offrent ainsi majoritairement des fruités mûrs. Les huiles AOP de Nîmes et de Nyons, en France, aussi.

FRUITÉ NOIR
Des arômes complexes

Le fruité noir, enfin, est élaboré selon une méthode ancestrale qui nécessite un début de fermentation des olives dans des conditions contrôlées (oxygène, temps et température). Il en résulte une huile crémeuse, aux arômes particuliers de cacao, de champignons et de sous-bois, appréciée de certains amateurs. Néanmoins, toute trace de fermentation constituant, vis-à-vis de la réglementation européenne, un défaut organoleptique, ce type d'huile est classé en «vierge», et non en «vierge extra». Catégorie plus rare, le fruité noir est, par exemple, caractéristique de l'AOP Provence.

L'AMER ET LE PIQUANT
Des signes de qualité

Deux autres attributs contribuent positivement à la saveur d'une huile d'olive: l'amer et le piquant. L'amertume, que l'on ressent sur l'arrière de la langue, est due à la présence naturelle de polyphénols. Le piquant (ou ardence) se caractérise par une sensation légèrement poivrée dans la gorge lors de la dégustation. Ces indicateurs de qualité révèlent la fraîcheur et les bienfaits nutritionnels (richesse en antioxydants) d'une huile. Au contraire, des goûts tels que le ranci (odeur et goût âcres, signe d'une mauvaise conservation), le moisi (goût désagréable indiquant un stockage dans des conditions trop humides) ou le chômé (flaveur déplaisante causée par une fermentation anaérobie avancée d'olives entassées ou mal entreposées) constituent des défauts majeurs. Une bonne huile se distingue par un bon équilibre entre le fruité, l'amer et le piquant. ■

« À consommer de préférence avant… »

La mise en bouteilles détermine la date optimale de consommation d'une huile d'olive. Mais cette information n'est pas la plus pertinente pour le client, auquel on devrait aussi indiquer l'année de récolte… Ce qui est, hélas, rarement le cas.

Pour garantir un produit loyal jusqu'au bout de sa commercialisation, une huile d'olive « vierge extra » doit être d'une qualité irréprochable au moment de son embouteillage, afin de minimiser sa dégradation lors du vieillissement. Il faut aussi qu'elle arbore une date de durabilité minimale (DDM) raisonnable, de manière à réduire l'impact des altérations liées au stockage de ce produit fragile. Cette date, qui se résume en général par la mention «à consommer de préférence avant…», permet de connaître la période pendant laquelle le produit conserve ses qualités gustatives, nutritives et organoleptiques optimales, sachant qu'il reste consommable sans danger après, mais avec un goût un peu moins bon, par exemple. La DDM est obligatoire >>

Les huiles sont à consommer en un ou deux ans, et à conserver dans un endroit sec et frais.

A. LECOMTE

>> et annonce une durée précise où l'huile conserve toutes ses qualités. Mais attention, fixé par les fabricants eux-mêmes, ce temps varie, selon les marques, d'un à deux ans à compter de la mise en bouteilles. De plus, il n'est pas calculé à partir de l'année de récolte, mais de celle de l'embouteillage. Or, beaucoup d'articles de grande consommation mélangent des huiles de millésimes différents. On peut ainsi trouver une huile composée à 15 % d'olives récoltées en 2021, à 30 % d'olives de 2022 et le reste de 2023, avec une date limite affichée en fonction de la date de mise en bouteilles ! En outre, les DDM les plus longues ne sont pas forcément le signe de produits impeccables. De fait, contrairement au vin, l'huile d'olive vieillit mal.

À utiliser assez rapidement

Seule garantie pour le consommateur : l'indication de la date de récolte des olives, malheureusement rarement précisée sur les bouteilles, et habituellement réservée aux huiles très haut de gamme. Dans tous les cas, mieux vaut consommer l'huile d'olive au cours de son année de production, et dans les trois ou quatre mois après l'ouverture de la bouteille. On doit aussi la conserver dans un endroit frais et sec, à l'abri de la lumière et de la chaleur, car elle est très sensible à l'oxydation et au rancissement qui en résulte. Afin de le limiter, il est préférable d'utiliser un huilier, par exemple en grès, dans lequel transvaser la quantité d'huile dont on a besoin pour manger ou cuisiner, et de laisser la bouteille à l'abri dans un placard.

Petit mémo

- **L'huile d'olive est très réglementée** (qualité, pays d'origine, date de durabilité minimale…).
- **Il ne faut pas se fier au packaging** (couleurs provençales, édition limitée, rameaux d'oliviers…).
- **C'est par un procédé mécanique** (pression ou centrifugation à froid) que doit être obtenue l'huile d'olive « vierge extra », sans traitement chimique ni chauffage susceptible d'altérer sa qualité. Cette mention de qualité supérieure est strictement encadrée par des tests organoleptiques et des analyses physicochimiques.
- **L'huile d'olive ne se bonifie pas en vieillissant.** Au contraire, elle baisse en qualité à partir de son pressage, plus ou moins vite selon sa qualité de départ.
- **Les tarifs vont de 5 à 50 € le litre,** mais la majeure partie de l'offre se situe entre 7 et 15 € le litre.
- **Pour cuisiner, pas besoin d'une huile « vierge extra »,** une « vierge » suffit largement.

Interview

PERRINE NADAUD *Adjointe au chef de l'Unité d'évaluation des risques liés à la nutrition de l'Anses**

« C'EST UNE SOURCE D'ÉNERGIE IMPORTANTE POUR NOTRE CORPS »

QC Quels bienfaits procure l'huile d'olive ?

Perrine Nadaud Elle contient de l'acide oléique, un acide gras mono-insaturé de la famille des oméga 9 qui représente une source importante d'énergie pour le corps. Quand l'apport en ces graisses remplace ceux des acides gras saturés, cela permet de maintenir des concentrations normales en cholestérol LDL – celui que l'on surnomme souvent le « mauvais cholestérol ». Ce dernier, lorsqu'il s'accumule dans les artères, peut favoriser la formation de plaques d'athérome à l'origine de maladies comme l'athérosclérose, mais également les AVC ou les infarctus. De plus, l'huile d'olive est riche en vitamine E, qui a des propriétés antioxydantes, et en vitamine K1, laquelle joue un rôle dans la coagulation sanguine.

QC Quelle différence pour la santé entre une huile « vierge extra », pressée à froid, et une version raffinée ?

P. N. Ce qui distingue l'huile d'olive « vierge extra » de celle raffinée, ce sont les teneurs en polyphénols, des antioxydants naturels, bien plus élevées dans la première. L'hydroxytyrosol, par exemple, préserve les cellules du stress oxydatif. Il protège aussi le cholestérol LDL contre les dommages de l'oxydation.

QC Faut-il n'utiliser que de l'huile d'olive, ou alterner avec d'autres huiles végétales, et lesquelles ?

P. N. L'une des recommandations de l'Anses est de diversifier ses consommations, notamment en alternant huile d'olive et huile de noix ou de colza. Cette dernière est également riche en oméga 3, peu consommés par la population française. De plus, elle a l'avantage d'être assez abordable. Les oméga 3 ne sont pas présents uniquement dans les huiles végétales; on les trouve dans certains poissons gras tels que le maquereau, le hareng ou le saumon. Favorisant la croissance comme le bon fonctionnement de nos cellules, les oméga 3 sont indispensables à notre organisme, qui ne peut les synthétiser. Il faut donc les ingérer via notre alimentation.

QC En dépit des bienfaits de l'huile d'olive, une surconsommation peut-elle avoir des effets délétères sur la santé ?

P.N. Bien sûr, tout excès est à éviter. Pour les apports journaliers, l'Anses recommande de consommer un poisson gras par semaine. En matière de quantité d'huile d'olive, et donc d'acide gras oléique, on parle de 15 à 20% de notre apport énergétique, soit deux à trois cuillères d'huile par jour, selon le site gouvernemental Mangerbouger.fr.

Propos recueillis par Pascale Barlet

**Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail.*

Laquelle pour la cui

Plébiscitée par les consommateurs, l'huile d'olive «vierge extra» est en principe un produit haut de gamme. Mais, dans cette catégorie, les niveaux de qualité diffèrent. Par ailleurs, il vaut mieux la réserver aux préparations froides.

Suave ou fruitée, fraîche ou longue en bouche, d'une grande finesse ou d'une rusticité intense… la palette gustative des huiles d'olive est très riche. Il en va donc de ce produit comme du vin. Son marché est très segmenté, du tout-venant aux grands crus. Très appréciée des consommateurs français, l'huile portant la mention «vierge extra» regroupe en principe le haut de gamme des huiles d'olive vierges, qui doivent obligatoirement être obtenues par pressage ou centrifugation mécanique, sans traitement chimique ni chauffage susceptible d'altérer leur qualité. Pour décrocher le qualificatif «extra», elles doivent également répondre à des critères chimiques et sensoriels précis, censés garantir, selon la formule consacrée, *«l'usage des meilleures olives et l'embouteillage des meilleures huiles»*. Pour autant, dans cette catégorie, les écarts de qualité entre produits demeurent importants. Et nos tests, année après année, déclassent une part non négligeable des huiles «vierge extra» en «vierge» – les trois quarts en 2025 !

À chacune son usage

Ainsi, une huile de Toscane produite à quelques dizaines d'hectolitres sur un terroir d'exception ou une huile catalane primée dans de prestigieux concours internationaux peuvent dépasser les 50 €/l,

Une huile d'olive vierge suffit pour la cuisson, car les arômes sont détruits par la chaleur.

FCAFOTODIGITAL/ISTOCK ; BANU SEVIM ; JONATHAN/ADOBE STOCK

sine ?

quand le prix plancher des références industrielles commence à 4 ou 5 €/l. Ces dernières ne sont pas forcément de mauvaise qualité. Cependant, elles manquent souvent de caractère, car elles résultent d'assemblages de plusieurs huiles provenant de régions (voire de pays) et de variétés différentes, afin d'obtenir une qualité et un goût acceptables du plus grand nombre mais uniformisé. Elles conviennent parfaitement pour la cuisson, car la chaleur détruit la plupart des arômes de l'huile. Nul besoin, par conséquent, d'utiliser une huile «vierge extra» si elle doit être chauffée: une huile vierge – moins riche en goût, toutefois tout aussi sûre d'un point de vue sanitaire – suffit largement pour cet usage. On a donc intérêt à avoir plusieurs huiles dans son placard, l'une, basique, destinée aux plats chauds, et d'autres, plus subtiles, que l'on appréciera pleinement sur des préparations crues.

Sachez aussi que l'huile d'olive est un ingrédient polyvalent qui, grâce à sa richesse aromatique, peut être employé de diverses façons en cuisine. Il sera possible de l'utiliser pour des assaisonnements et des vinaigrettes bien sûr, mais également pour des marinades de viande ou de poisson, des cuissons douces à basse température (confit, légumes, viande…) ou d'autres classiques au four jusqu'à 210 °C, ou encore en finition afin de rehausser un plat (pâtes, légumes, soupe…). Et même en pâtisserie, à la place du beurre, afin d'apporter légèreté, moelleux et note parfumée.

Nutrition, santé et régime crétois

Enfin, impossible de parler huile d'olive sans évoquer son aspect santé. À l'instar de celles d'arachide et de tournesol oléique (variété de tournesol), les huiles d'olive sont composées en majorité de lipides mono-insaturés, aussi appelés oméga 9. Ces acides gras, neutres pour l'organisme, leur procurent une résistance aux hautes températures qui les rend stables à la cuisson, même en friture. Par contre, l'huile d'olive n'est pas particulièrement riche en acides gras oméga 3. Elle reste néanmoins recommandée par les autorités sanitaires en raison de son effet positif sur la santé. Peut-être grâce à ses teneurs élevées en acide oléique et en antioxydants, et plus particulièrement en polyphénols, tocophérols et vitamine E (lire aussi l'interview p. 123). Cette réputation lui vaut également d'être l'un des piliers du régime crétois (ou régime méditerranéen), lequel réduit les risques d'infarctus, d'AVC et de diabète de type 2, comme de cancers, de maladies inflammatoires, etc. ■

LABEL BIO Il ne donne pas plus de goût

Le label Agriculture biologique (AB) est de plus en plus présent sur les huiles vendues en grandes surfaces. Mais attention, si cette certification garantit l'absence de traitement chimique des olives, donc a priori l'absence de résidus de pesticides, elle n'a pas d'impact sur la qualité gustative de l'huile, ni sur la présence des autres polluants recherchés par *Que Choisir* lors de ses tests, à savoir les huiles minérales et certains plastifiants comme les phtalates. Notons que les huiles d'olive conventionnelles affichent habituellement des taux de contamination aux pesticides assez bas par rapport aux autres cultures fruitières ou légumières.

PRIX DE L'ÉLECTRICITÉ

Un coût du nucléaire à fort enjeu

À partir du 1er janvier 2026, un nouveau dispositif de tarification de l'électricité va s'appliquer. Il repose sur une estimation du coût de production du nucléaire historique en France. Mais ce calcul est-il juste ?

Un peu plus de 60 € – 60,30 €, pour être précis – le mégawattheure (MWh): la Commission de régulation de l'énergie (CRE) française a publié son évaluation du coût complet de production d'électricité par les réacteurs nucléaires d'EDF sur la période 2026-2028, prenant en compte toutes les installations autorisées à en produire avant janvier 2026. Ce parc «historique» en comprend 57, dont le réacteur pressurisé européen (EPR) raccordé au réseau en décembre 2024, Flamanville 3. Or ce coût de production du nucléaire existant s'avère très proche de celui qu'elle avait estimé en 2023 (60,70 €/MWh). Emmanuelle Wargon, la présidente de la CRE, avait pourtant récemment annoncé s'attendre à une évaluation autour de *«66 ou 67 €/MWh»,* en intégrant l'inflation des dernières années sur les charges d'EDF, rappelle le quotidien économique *Les Échos.* Mais d'autres facteurs, notamment un changement de méthodologie, ont finalement eu un impact baissier, explique-t-elle.

Changement de modèle

Il faut dire que l'estimation de la CRE est cruciale dans le fonctionnement du versement nucléaire universel (VNU), le dispositif qui succédera, le 1er janvier 2026, à l'actuel Accès régulé à l'électricité nucléaire historique (Arenh). Pour rappel, ce dernier a été instauré en juillet 2011 pour *«partager la rente nucléaire»* au moment de l'ouverture à la concurrence du marché de l'électricité. Dans ce cadre, EDF devait vendre jusqu'à 100 térawattheures (TWh) par an – soit environ un tiers de sa production d'électricité nucléaire – à des fournisseurs alternatifs, au prix très avantageux pour ces derniers de 42 €/MWh. Changement de système à compter de janvier 2026: EDF commercialisera désormais la totalité de son électricité d'origine nucléaire sur les marchés, dont les cours sont instables et beaucoup plus élevés (autour de 62 €/MWh ces temps-ci). Une telle évolution laisse craindre une explosion des coûts de l'électricité pour les ménages, dont l'UFC-Que Choisir s'est fait l'écho dans une étude publiée en février dernier.

Deux seuils de taxation fixés

En contrepartie, la nouvelle régulation prévoit une taxation des profits réalisés par EDF sur la vente sur les marchés de gros de sa production électronucléaire, et une redistribution des gains (le VNU) aux consommateurs d'électricité. Avec deux seuils: l'un dit de «taxation», l'autre, d'«écrêtement». Lorsque EDF écoulera son électricité à un tarif compris entre les deux, les bénéfices de la vente seront imposés à hauteur de 50%. Au-delà du seuil d'écrêtement, ils le seront à 90%. Reste à déterminer ces niveaux à partir desquels les taxes se déclencheront… C'est là que le calcul de la CRE revêt son importance. Le seuil de taxation s'activera quand EDF commercialisera son électricité nucléaire entre 5 et 25 €/MWh au-dessus du coût complet estimé par la CRE (60,30 €/MWh, donc, sur la période 2026-2028). Même logique pour le seuil d'écrêtement, mais avec une fourchette plus haute: de 35 à 55 €/MWh. D'ici à la fin de l'année, par un décret, le gouvernement devra préciser où il place le curseur au sein de ces deux fourchettes.

Fabrice Pouliquen

IMPÔTS 2026

Quelques conseils pour les réduire

Vous cherchez à payer moins d'impôts ? C'est possible. Toutefois, pour profiter de tel ou tel avantage fiscal promis, il faut en maîtriser le fonctionnement et en connaître les limites. Explications.

Certaines dépenses payées en 2025 seront partiellement déductibles de vos impôts de 2026. Ainsi, vous aurez droit à une réduction d'impôt si vous faites un don aux Restos du cœur, investissez dans l'immobilier locatif en Denormandie ou souscrivez des parts de PME. Et vous bénéficierez d'un crédit d'impôt si vous employez un salarié à domicile, confiez votre petit dernier à une crèche ou installez une recharge pour véhicule électrique chez vous. Dès lors, pour optimiser ces bonus, sélectionnez vos outils de défiscalisation avec méthode. D'autant que la prochaine loi de finances, en préparation, pourrait faire disparaître plusieurs avantages… En attendant, vous en profiterez de toute façon sur les dépenses réalisées jusqu'au 31 décembre 2025, les suppressions ne s'appliquant qu'à celles réglées à compter du 1er janvier 2026.

Les bonus remboursables et les autres

Pour une même dépense, une même baisse d'impôt est attribuée à tous les foyers. Cette dernière ne dépend pas du taux d'imposition des contribuables, contrairement à celles procurées par les charges déductibles des revenus (versements sur un PER, pension alimentaire allouée à son parent dans le besoin…). Si vous engagez des frais ouvrant droit à des réductions et des crédits d'impôt, le fisc commencera par imputer les premières sur vos impôts de 2026, puis les seconds sur les impôts restants. Cependant, les réductions seront prises en compte uniquement dans la limite du montant de vos impôts. La fraction excédentaire sera perdue et il ne sera pas possible de l'imputer sur les années suivantes. Au contraire, si vos crédits dépassent vos impôts diminués de vos réductions, le fisc vous restituera l'excédent. Résultat, si vous ne payez que peu d'impôts – et a fortiori si vous n'êtes pas imposable –, privilégiez les dépenses ouvrant droit à un crédit plutôt qu'à une réduction d'impôt, afin de profiter à plein des avantages fiscaux. La part des bonus qui dépasse vos impôts 2026 vous sera remboursée l'été prochain. Bonne nouvelle, les dépenses «contraintes» (frais d'emploi à domicile, de garde d'enfant, de travaux réalisés dans le logement, etc.) ouvrent généralement droit à un crédit d'impôt remboursable. En revanche, celles «choisies» (don à une association, souscription de parts de PME, investissement locatif…) sont, le plus souvent, assorties d'une simple réduction d'impôt.

Olivier Puren

Bon à savoir

Les frais de séjour en Ehpad ne conduisent qu'à une réduction d'impôt, alors qu'il s'agit de dépenses contraintes très onéreuses… Seuls les séniors qui payent des impôts peuvent en bénéficier – ceux qui ne sont pas imposables n'ont droit à aucune aide du fisc.

QUE CHOISIR PRATIQUE LABELS, PRÉCISION

Concernant la marque de cosmétiques Natrue, citée dans le *QCP* n° 145 (p. 42), nous n'avons indiqué qu'un seul organisme de certification, alors qu'elle en compte huit : Bioagricert, Bio gro, Bio.inspecta, CCPB, Certisys, Eco control, Ecogruppo et QimalBD.

RIZ

De l'arsenic néfaste pour la santé

Peut-être ne le saviez-vous pas, mais le riz et l'eau de boisson contiennent des teneurs particulièrement élevées en arsenic. Or, cet élément présente des risques pour la santé.

L'arsenic est un élément naturel présent dans les roches, et libéré dans l'environnement lors de leur érosion. Il est alors susceptible de polluer les nappes phréatiques et les cours d'eau, donc les rizières – faisant du riz et de l'eau de boisson nos principales sources d'exposition alimentaire. L'arsenic est également rejeté dans l'eau et dans l'air par les activités industrielles, en particulier l'extraction minière, la métallurgie, la verrerie, le textile ou la papeterie. Sans oublier le tabac, qui en contient aussi en quantités non négligeables.

Tous les riz sont concernés

Très toxique sous sa forme minérale, l'arsenic peut provoquer des cancers (peau, vessie, poumon, etc.) et des lésions cutanées si on en ingère souvent, voire favoriser les maladies cardiovasculaires et le diabète. C'est, en outre, un perturbateur endocrinien probable. L'Organisation mondiale de la santé (OMS) le considère d'ailleurs comme *«l'une des 10 substances chimiques gravement préoccupantes pour [notre] santé»*.

Aucun des principaux pays producteurs de riz n'est épargné par cette pollution, et toutes les références de riz thaï et basmati de notre dernier comparatif (*QC* n° 650) en renferment. Les teneurs mesurées varient du simple au triple, et sont globalement plus élevées dans le riz thaï. Néanmoins, toutes restent dans la limite réglementaire – il faut alors déterminer si cette dernière est réellement protectrice pour les consommateurs. Cela étant, comme les Français ne mangent qu'environ 5 kg de riz par an (ce qui est peu), le risque sanitaire est moindre.

NOTRE CONSEIL Nettoyez bien le riz avant la cuisson et rincez-le de nouveau après. Cela élimine près de la moitié de l'arsenic présent, ainsi que les résidus de pesticides et de poussières.

Elsa Casalegno

NOS ASSOCIATIONS LOCALES

L'UFC-Que Choisir compte 131 associations locales en France, animées par des militants bénévoles. Ces antennes fournissent à leurs adhérents des conseils juridiques et techniques ainsi que de la documentation sur des questions de vie quotidienne.

01 AIN
• Maison de la culture
et de la citoyenneté
CS 70270
4, allée des Brotteaux
01006 BOURG-
EN-BRESSE CEDEX
04 74 22 58 94

02 AISNE
• 31 bis, rue du Gal-Patton
02880 CROUY
09 70 96 64 93

03 ALLIER
• 52, rue de la Gironde
03100 MONTLUÇON
04 70 05 30 38
• 42, rue du Progrès
03000 MOULINS
04 70 20 96 30

04 ALPES-DE-HAUTE-PROVENCE
• 22, rue d'Aubette
04100 MANOSQUE
04 92 72 19 01

07 ARDÈCHE
• Maison des associations
11, avenue de la Gare
07200 AUBENAS
04 75 39 20 44

08 ARDENNES
• BP 561
5, rue Jean-Moulin
08000 CHARLEVILLE-
MÉZIÈRES CEDEX
03 24 53 70 17

09 ARIÈGE
• Maison de la citoyenneté
16, rue de la République
09200 SAINT-GIRONS
05 61 66 03 66

11 AUDE
• 118, route d'Amissan
11000 NARBONNE
04 68 32 68 72

12 AVEYRON
• Maison des associations
15, avenue Tarayre
12000 RODEZ
05 65 77 00 01

13 BOUCHES-DU-RHÔNE
• Le Félibrige, bât. B
4, place Coimbra
13090 AIX-EN-PROVENCE
04 42 93 74 57
•11 bis, rue Saint-Ferréol
13001 MARSEILLE
04 91 90 05 52
• 8, boulevard Joliot-Curie
13500 MARTIGUES
04 42 81 10 21
• 6, rue des Grands-Prés
13300 SALON-DE-PROVENCE
04 90 42 19 80

14 CALVADOS
• 19, quai de Juillet
14000 CAEN
02 31 86 32 54

15 CANTAL
• BP 17
19, rue de la Coste
15018 AURILLAC
04 71 48 58 68

16 CHARENTE
• Immeuble George-Sand
83, avenue
de Lattre-de-Tassigny
16000 ANGOULÊME
05 45 95 32 84

17 CHARENTE-MARITIME
• 3, rue J.-B.-Charcot
17000 LA ROCHELLE
05 46 41 53 42

18 CHER
• Maison des associations
28, rue Gambon
18000 BOURGES
02 48 70 48 02

19 CORRÈZE
•13, rue Émile-Duclaux
19100 BRIVE-LA-GAILLARDE
05 55 23 19 37

20 CORSE
• Le Golo, bât. A
Av. de l'Aspirant-Michelin
20090 AJACCIO
04 95 22 69 83

21 CÔTE-D'OR
• Maison des associations
2, rue des Corroyeurs
(boîte n° 14)
21000 DIJON
03 80 43 84 56

22 CÔTES-D'ARMOR
• Espace Volta, bât. B
1, rue André-Marie-Ampère
22300 LANNION
02 96 46 66 09
• 3, rue Pierre-Cléret
22120 YFFINIAC
02 96 78 12 76

23 CREUSE
• BP 242
11, rue Braconne
23005 GUÉRET CEDEX
05 55 52 82 83

24 DORDOGNE
• 1, square Jean-Jaurès
24000 PÉRIGUEUX
05 53 09 68 24

25 DOUBS
• 8, avenue de Montrapon
25000 BESANÇON
03 81 81 23 46

26 DRÔME
• 41, avenue Sadi-Carnot
26000 VALENCE
04 75 42 58 29

27 EURE
• Immeuble Cambrésis
17, rue des Aérostiers
27000 ÉVREUX
02 32 39 44 70

28 EURE-ET-LOIR
• La Madeleine
25, place Saint-Louis
28000 CHARTRES
02 37 30 17 57

29 FINISTÈRE
• Maison
des associations
6, rue Pen-Ar-Creac'h
29200 BREST
02 98 80 64 30
• 3, allée de Roz-Avel
29000 QUIMPER
02 98 55 30 21

30 GARD
• 20, rue du Cdt-Audiber
30100 ALÈS
04 66 52 80 80
• Bât. A
65, avenue Jean-Jaurès
30900 NÎMES
04 66 84 31 87

31 HAUTE-GARONNE
• Siège social
BP62201
31320 CASTANET CEDEX
07 80 01 68 72
• Ass. locale de Toulouse
59, boulevard Lascrosses
31000 TOULOUSE
05 61 22 13 00

32 GERS
• 44, rue Victor-Hugo
32000 AUCH
05 62 61 93 75

33 GIRONDE
• 17, cours
Balguerie-Stuttenberg
33300 BORDEAUX
05 56 79 91 94

34 HÉRAULT
• Maison Daniel-Cordier
Boîte aux lettres n° 15
2, rue Jeanne-Jugan
34500 BÉZIERS
04 67 28 06 06
• BP 2114
3, rue Richelieu
34026 MONTPELLIER CEDEX 1
04 67 66 32 96
• BP 106
53, boulevard
Chevalier-de-Clerville
34207 SÈTE CEDEX
04 30 41 53 30

35 ILLE-ET-VILAINE
• 8, place du Colombier
35000 RENNES
02 99 85 94 23
• Saint-Malo et ses environs
8E avenue de Moka
35400 SAINT-MALO
02 99 56 80 47

36 INDRE
• 34, espace Mendès-France
Avenue François-Mitterrand
36000 CHÂTEAUROUX
02 54 27 43 57

37 INDRE-ET-LOIRE
• 12, rue Camille-Flammarion
37000 TOURS
02 47 51 91 12

38 ISÈRE
• 8, rue brigadier Megevand
38300 BOURGOIN-JALLIEU
04 74 28 02 53
• 24 bis, rue Mallifaud
38100 GRENOBLE
04 76 46 88 45

39 JURA
• 3A, avenue Aristide-Briand
(adresse de visite)
• 27, rue de la Sous-
Préfecture (adresse postale)
39100 DOLE
03 84 82 60 15

40 LANDES
• Association Camille-Pédarré
89 bis, rue Martin-Luther-King
40000 MONT-
DE-MARSAN
05 58 05 92 88

41 LOIR-ET-CHER
• Maison des associations
17, rue Roland-Garros
41000 BLOIS
02 54 42 35 66

42 LOIRE
• 17, rue Brossard
42000 SAINT-ÉTIENNE
04 77 33 72 15

43 HAUTE-LOIRE
• 29, boulevard
Dr Chantemesse
43000 AIGUILHE
04 71 02 29 45

44 LOIRE-ATLANTIQUE
• Maison des associations
2 bis, rue Albert-de-Mun
44600 SAINT-NAZAIRE
02 40 22 00 19
• 1, place du Martray
44000 NANTES
09 53 75 15 94

45 LOIRET
• 39, rue Saint-Marceau
45000 ORLÉANS
02 38 53 53 00
• Maison des associations
32, rue Claude-Debussy
45120 CHALETTE-
SUR-LOING
09 62 03 03 42

46 LOT
• Espace associatif
Place Bessières
46000 CAHORS
05 65 53 91 19

47 LOT-ET-GARONNE
• BP 50301
159, avenue Léon-Blum
47008 AGEN
05 53 48 02 41

49 MAINE-ET-LOIRE
• Espace Frédéric-Mistral,
4, allée des Baladins
49000 ANGERS
02 41 88 56 42

50 MANCHE
• 167, rue Gal-Gerhardt
50000 SAINT-LÔ
02 33 05 68 76

51 MARNE
• Espace entreprises
Saint-John-Perse
2, cour du Gal-Eisenhower
51100 REIMS
03 26 08 63 03

NOS ASSOCIATIONS LOCALES

52 HAUTE-MARNE
• 14, rue de Vergy
52100 SAINT-DIZIER
03 25 56 26 59

53 MAYENNE
• 31, rue Oudinot
53000 LAVAL
02 43 67 01 18

54 MEURTHE-ET-MOSELLE
• 76, rue de La-Hache
54000 NANCY
09 52 19 48 23

56 MORBIHAN
• Maison des familles
2, rue du Pr-Mazé
56100 LORIENT
02 97 84 74 24

57 MOSELLE
• BP 46
1A, impasse de l'École
57470 HOMBOURG-HAUT
03 87 81 67 80
• Association locale
BP 40103
57951 MONTIGNY-LÈS-METZ
03 72 13 73 57
• 2, rue d'Austrasie
57100 THIONVILLE
03 82 51 84 29

58 NIÈVRE
• 2 bis, boulevard
Jacques-Duclos
58000 NEVERS
03 86 21 44 14

59 NORD
• 104, rue d'Esquerchin
59500 DOUAI
03 27 96 05 15
• Terreplein du Jeu de mail
Rue du 11-Novembre-1918
59140 DUNKERQUE
06 16 42 49 10
• 54, rue Jacquemars-Gielée
59000 LILLE
03 20 85 14 66
• Maison des associations
Faubourg-Saint-Quentin
BP40037
13, rue du Progrès
59600 MAUBEUGE
06 47 49 53 81

60 OISE
• BP 80059
60303 SENLIS CEDEX

61 ORNE
• MVA
25, rue Demées
61000 ALENÇON
02 33 26 79 47

62 PAS-DE-CALAIS
• Maison des sociétés
Bureaux 39 à 42
16, rue Aristide-Briand
62000 ARRAS
03 21 23 22 97
• Maison des associations
Élie-Vignon
1, place du Gal-de-Gaulle
62219 LONGUENESSE
03 21 39 81 81

63 PUY-DE-DÔME
• 21, rue Jean-Richepin
63000 CLERMONT-FERRAND
04 73 98 67 90
• Maison des associations
20, rue du Palais
63500 ISSOIRE
04 73 55 06 76

64 PYRÉNÉES-ATLANTIQUES
• 9, rue Sainte-Ursule
64100 BAYONNE
05 59 59 48 70
• 10, rue du Pt-Kennedy
64300 ORTHEZ
05 59 67 05 80
• 16, rue du Cne-Guynemer
64000 PAU
05 59 90 12 67

65 HAUTES-PYRÉNÉES
• 4, rue Alphonse-Daudet
65000 TARBES
09 62 34 21 21

66 PYRÉNÉES-ORIENTALES
• 45, avenue Marcelin Albert
66000 PERPIGNAN
09 83 87 07 07

67 BAS-RHIN
• 1A, place
des Orphelins
67000 STRASBOURG
03 88 37 31 26

68 HAUT-RHIN
• 4, avenue Clémenceau
68100 MULHOUSE

69 RHÔNE
• 1, rue Sébastien-Gryphe
69007 LYON
04 78 72 00 84

70 HAUTE-SAÔNE
• BP 10357
22, rue du Breuil
70006 VESOUL
03 84 76 36 71

71 SAÔNE-ET-LOIRE
• 2, rue Jean-Bouvet
71000 MÂCON
03 85 39 47 17

72 SARTHE
• 21, rue Besnier
72000 LE MANS
02 43 85 88 91

73 SAVOIE
• 23 BP 10427
25, boulevard des Anglais
73104 AIX-LES-BAINS
07 83 74 12 73
• Maison des associations
21, rue Georges-Lamarque
73200 ALBERTVILLE
04 79 37 11 01
• 67, rue Saint-François-de-Sales
73000 CHAMBÉRY
04 79 85 27 87

74 HAUTE-SAVOIE
• 48, rue des Jardins
74000 ANNECY
04 50 69 74 67

75 PARIS
• 54, rue de l'Ouest
75014 PARIS
01 56 68 97 48

76 SEINE-MARITIME
• 36, rue du Mal-Joffre
76600 LE HAVRE
09 62 51 94 37
• 12, rue Jean-Lecanuet
76000 ROUEN
02 35 70 27 32

77 SEINE-ET-MARNE
• 22, rue du
Palais-de-Justice
77120 COULOMMIERS
01 64 65 88 70
• Centre social
et culturel Brassens
4, patio des Catalpas
77420 CHAMPS-SUR-MARNE
01 64 73 52 07

78 YVELINES
• 3, avenue des Pages
78110 LE VÉSINET
06 08 90 20 16
• 7, avenue Foch
78120 RAMBOUILLET
01 78 82 52 12
• 5 bis, Grande-Rue
78480 VERNEUIL-SUR-SEINE
01 39 65 63 39• 5, impasse
des Gendarmes
78000 VERSAILLES
01 39 53 23 69

79 DEUX-SÈVRES
• Hôtel de la vie associative
12, rue Joseph-Cugnot
79000 NIORT
05 49 09 04 40

80 SOMME
• 5, rue Pasteur
80480 SALOUEL
03 22 72 10 84

81 TARN
• 3, place du Palais
81000 ALBI
05 63 38 42 15

82 TARN-ET-GARONNE
• BP 397
25, place Charles-Caperan
82000 MONTAUBAN
05 63 20 20 80

83 VAR
• 1196, boulevard de la Mer
83616 FRÉJUS
09 63 04 60 44
• L'oiseau de feu
113, rue Henri Poincaré
83000 TOULON
04 94 89 19 07

85 VENDÉE
• 8, boulevard Louis-Blanc
85000 LA-ROCHE-SUR-YON
02 51 36 19 52

86 VIENNE
• 1, rue du 14 juillet 1789
86000 POITIERS
09 87 76 39 91

87 HAUTE-VIENNE
• 4, cité Louis-Casimir-Ranson
87000 LIMOGES
05 55 33 37 32

88 VOSGES
• Maison des associations
BP 1004
6, quartier Magdeleine
88050 ÉPINAL CEDEX 9
03 29 64 16 58

89 YONNE
• 12, boulevard Vaulabelle
89000 AUXERRE
03 86 51 54 87

91 ESSONNE
• La Ferme
91800 BOUSSY-SAINT-ANTOINE
01 69 56 02 49
• Val d'Orge
Place du 19-Mars-1962
91240 SAINT-MICHEL-SUR-ORGE
09 67 19 08 13

92 HAUTS-DE-SEINE
• BP 56
92145 CLAMART CEDEX
07 61 07 64 97
• Siège de l'AL
11, rue Hédouin
92190 MEUDON
• BP 60025
92276 BOIS-COLOMBES CEDEX
• Maison de l'Amitié
18, rue des Écoles
92210 SAINT-CLOUD
06 41 06 59 35
• Mairie de Sèvres
54, Grande-Rue
92310 SÈVRES

93 SEINE-SAINT-DENIS
• 19, rue Jules-Guesde
93140 BONDY
06 42 01 07 89
• Centre Salvador-Allende
2, avenue du Dauphiné
93330 NEUILLY-SUR-MARNE

94 VAL-DE-MARNE
• Centre social Kennedy
36, boulevard J.-F.-Kennedy
94000 CRÉTEIL
01 43 77 60 45
• Centre Marius-Sidobre
26, rue Émile-Raspail
94110 ARCUEIL
01 45 47 74 74

95 VAL-D'OISE
• Espace Nelson-Mandela
82, boulevard du Gal-Leclerc
95100 ARGENTEUIL
01 39 80 78 15
• BP 90001
95471 FOSSES CEDEX
01 34 72 76 87
• Office culturel du Forum
Place François-Truffaut
95210 SAINT-GRATIEN
07 71 71 09 73

LA RÉUNION
• Résidence Les Vacoas
7, rue Paul-Demange
97480 SAINT-JOSEPH
02 62 45 24 44

NOUVELLE-CALÉDONIE
• Résidence du Vallon d'Argent
BP 2357
82, rue Capiez
98846 NOUMÉA CEDEX
06 87 28 51 20

NE REFERMEZ PAS CE NUMÉRO PRATIQUE...

**... sans avoir découvert l'expertise de nos autres publications.
Toute l'année, nous veillons à apporter une information indépendante, pratique et utile pour la défense du consommateur.**

SAVOIR CE QUE L'ON CONSOMME, C'EST CONSOMMER INTELLIGENT

QUE CHOISIR

▶ Chaque mois

Que Choisir vous tient au fait de l'actualité de la consommation. Il informe, teste, analyse et compare. Il prend parti, recommande ou dénonce.

Commandez les derniers numéros parus au prix unitaire de 5 €.

NOUVEAU QUE CHOISIR Budgets !

▶ Chaque trimestre

Succédant à *Que Choisir Argent,* ce hors-série est orienté « dépenses au quotidien ». Réponses, conseils et mises en garde vous attendent via un dossier central, des décryptages, des enquêtes de terrain... sans oublier votre cahier argent.

Commandez les derniers numéros parus au prix unitaire de 5,20 €.

Pour commander les anciens numéros et vous abonner, mais aussi connaître les sommaires détaillés, les dossiers abordés ou encore les tests réalisés...

WWW.QUECHOISIR.ORG

ou flashez ce QR code

LES SUPERMARCHÉS DRIVES
LES MOINS CHERS

UFC QUE CHOISIR

Union Fédérale
des Consommateurs
– Que Choisir

F8/ADOBE STOCK

Comparez les prix

Grâce à **notre carte interactive,**
localisez les magasins drives
proches de chez vous
et maîtrisez votre budget courses

Ufcqc.link/supermarche146

Un service gratuit !

Pour accéder
à la carte,
copiez l'URL
ci-dessus
ou flashez
le QR code