QUE CHOISIR
EXPERT • INDÉPENDANT • SANS PUBLICITÉ

QUE CHOISIR pratique

Numéro 136 • Juin 2023 • 6,95 € • ISSN 1773-9713

NUMÉRIQUE

SÉCURISEZ VOS DONNÉES !

- Protéger sa vie privée
- Réagir en cas de fraude

Test 37 LOGICIELS *gratuits ou payants*

ENQUÊTE Les Français notent leur assurance habitation

DOM surface: 8,20 € TOM: 960 XPF
L 13463 - 136 - F: 6,95 € - RD

QUE CHOISIR PRATIQUE Numéro 136 • JUIN 2023
NUMÉRIQUE SÉCURISEZ VOS DONNÉES !

Édito

VOS DONNÉES VALENT DE L'OR

Ces dernières années, les hôpitaux français ont été la cible de cyberattaques. Deux raisons principales à cela: la vulnérabilité de leurs réseaux informatiques et la grande valeur, sur le darknet, des milliers d'informations personnelles qu'ils contiennent. Au centre hospitalier de Corbeil-Essonnes, dans le sud francilien, personnel et patients se remettent tout juste de l'offensive, deux ans après. Les pirates ont d'abord bloqué le système informatique, avant de demander une rançon colossale. Face au refus de payer de l'établissement, ils ont divulgué les données de centaines de personnes sur la Toile… Cet événement n'est, hélas, pas exceptionnel. Si ce qui touche à votre santé intéresse fortement les escrocs, il en va de même pour vos informations bancaires, vos comptes sur les réseaux sociaux, vos données administratives, etc. C'est un fait, le monde se numérise. Difficile d'échapper à cette tendance. En parallèle, les criminels sont de plus en plus organisés et professionnalisés. Face à ce fléau, il faut s'armer. Bonne nouvelle, des protections efficaces existent, qu'elles soient législatives ou techniques. *Que Choisir Pratique* a fait appel à Damien Bancal, spécialiste de la cybersécurité, pour vous indiquer les gestes à adopter, les bons outils à utiliser et vers qui se tourner en cas de problème. De quoi vous aider à reprendre le contrôle !

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 : 44 € ▪ 1 an + 4 hors-séries : 62 €
1 an + 4 hors-séries + 4 numéros *Que Choisir Pratique* : 90 €

IMPRESSION / COUVERTURE
BLG Toul, 2780, route de Villey-S[t]-Étienne 54200 TOUL

DISTRIBUTION MLP

COMMISSION PARITAIRE
n° 0722 G82318
Imprimé sur papier Perlen Value (Suisse)

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

Photos de couv. : Manolo82/Istock, Weerapat1003/Adobe Stock, Chocoflin/Adobe Stock

Sommaire

WEERAPAT1003/ADOBE STOCK

SOMMAIRE

Les obligations légales

La protection des données personnelles est devenue un enjeu majeur, en raison de leur importance croissante au quotidien et de l'augmentation de leur utilisation par des particuliers, des entreprises ou des États. Il s'agit d'informations telles que les numéros de téléphone, les historiques de navigation web, les adresses postales et de messagerie électronique… Ces datas peuvent être collectées par des sociétés privées et employées à des fins commerciales, ou récoltées par des organismes publics – les gouvernements ont alors la possibilité de s'en servir afin de surveiller les activités de leurs citoyens. Certaines personnes s'en procurent également, voire les volent, pour discriminer, harceler ou rançonner. Sécuriser vos données personnelles est donc impératif. Sinon, vous courez le risque qu'il en soit fait usage à votre insu, et à des fins pas forcément éthiques ni conformes à vos intérêts. Pas de panique, cependant : il existe plusieurs moyens de s'en défendre.

FILADENDRON/ISTOCK

L'EUROPE DÉFEND SES CITOYENS

Il a fallu 23 ans à la Commission européenne pour aboutir à la version actuelle du règlement sur la protection des données.

Le Règlement général sur la protection des données, communément appelé RGPD, s'applique dans les 27 États membres de l'Union européenne depuis 2018.

Cette loi, conçue pour protéger les libertés et droits fondamentaux des individus sur le traitement de leurs données à caractère personnel, découle d'une directive européenne adoptée en 1995. Entre-temps, 23 ans de cheminement et d'avancées progressives ont été nécessaires avant d'aboutir à la version actuelle du texte, comme le montre la frise chronologique ci-contre.

Aujourd'hui, le RGPD intensifie la responsabilisation et l'obligation de transparence des organisations en charge du traitement des données personnelles, et accroît les droits des personnes concernées. Les entreprises qui collectent, utilisent ou stockent ce type d'informations voient aussi leurs devoirs renforcés: obligation d'obtenir un consentement d'exploitation; de garantir le droit d'accès, d'effacement et de portabilité; de notifier les violations de données.

Des amendes qui peuvent être salées

Le non-respect de ces mesures peut entraîner des amendes jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel d'une société. Parmi les sanctions les plus marquantes de ces derniers mois, figure la condamnation du groupe Meta (maison mère de Facebook, WhatsApp et Instagram) à payer 390 millions d'euros. Une mesure adoptée par l'autorité irlandaise de protection des données le 31 décembre 2022, à la suite des décisions contraignantes du Comité européen à la protection des données (CEPD). ■

P. GRECAUD/ADOBE STOCK

Chronologie DES LOIS POUR RENFORCER LES DROITS

24 octobre 1995 Adoption de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

22 juin 2011 Publication, par le Contrôleur européen de la protection des données (CEPD), d'un avis sur la communication de la Commission européenne intitulé « Une approche globale de la protection des données à caractère personnel dans l'Union européenne ».

25 janvier 2012 Proposition par la Commission européenne d'une réforme globale des règles adoptées en 1995, afin de renforcer les droits en matière de respect de la vie privée dans l'environnement en ligne.

7 mars 2012 Adoption par le CEPD d'un avis sur le train de réformes présenté par la Commission européenne.

23 mars 2012 Adoption par le groupe de travail « Article 29 » d'un avis sur la proposition de réforme de la protection des données.

5 octobre 2012 Apport d'une contribution supplémentaire au débat sur la réforme de la protection des données par le groupe de travail « Article 29 ».

12 mars 2014 Adoption par le Parlement européen du Règlement général sur la protection des données (RGPD).

27 juillet 2015 Publication par le CEPD de ses recommandations aux colégislateurs européens responsables de la négociation de la version finale du règlement général, sous la forme de suggestions d'ordre rédactionnel. Il lance aussi une application mobile permettant de comparer la proposition de la Commission avec les derniers textes du Parlement et du Conseil.

15 décembre 2015 Accord entre le Parlement européen, le Conseil et la Commission sur le règlement général.

2 février 2016 Publication d'un plan d'action pour la mise en œuvre du règlement général, dont le droit à la portabilité des données par le groupe de travail « Article 29 ».

27 avril 2016 Publication au *Journal officiel* de l'Union européenne du règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

24 mai 2016 Entrée en vigueur du règlement (UE) 2016/679.

10 janvier 2017 Publication de deux nouveaux règlements, sur la vie privée et les communications électroniques ainsi que sur la protection des données au sein des institutions européennes.

6 mai 2018 Transposition, dans les législations nationales, de la directive européenne sur la protection des données.

22 mai 2018 Proposition de règlement du Parlement européen et du Conseil sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et agences de l'Union et sur la libre circulation de ces données, abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE [première lecture].

25 mai 2018 Rectificatif au règlement (UE) 2016/679 du 27 avril 2016 et entrée en vigueur du Règlement général sur la protection des données (RGPD).

NOUN PROJECT

LA PHILOSOPHIE DU RGPD

Ce règlement aura fait couler beaucoup d'encre avant son entrée en vigueur. Le plus compliqué : garantir que les données personnelles des citoyens soient traitées de manière éthique et transparente.

Le règlement général sur la protection des données (RGPD) repose sur plusieurs principes. D'abord, les individus ont le droit à la protection de leurs informations personnelles. Ensuite, les entreprises, les administrations et les associations – bref, toute organisation privée ou publique et ses sous-traitants –, quelles que soient leur taille et leur activité, ont la responsabilité de la garantir. Ce texte définit clairement les contours légaux de la collecte, du stockage et du traitement des datas de chacun. Il fixe également un cadre juridique en matière de transparence, de confidentialité et de notification en cas de violation de leur sécurité. Tous les acteurs concernés sont contraints de s'adapter à ces exigences afin d'assurer les droits des citoyens de l'Union européenne dont les données sont récoltées.

Parmi ces droits, examinons celui à l'effacement, dit aussi «à l'oubli»: toute personne physique a la possibilité de demander à n'importe quelle structure détenant des données personnelles de faire disparaître de son référencement une information erronée, fausse ou malveillante se rapportant à elle. Un moteur de recherche ou un commerçant doivent être capables de fournir tous les renseignements qu'ils possèdent sur vous afin qu'ils soient modifiés, détruits ou récupérés par d'autres entités. Pour cela, entreprises et organisations sont tenues d'adopter des politiques et des procédures adéquates, de former leur personnel et de renforcer la sécurisation de leurs dispositifs de traitement des données.

LES RÈGLES QUI DOIVENT ÊTRE SUIVIES

Le RGPD a défini un certain nombre d'obligations que tout acteur privé ou public recueillant des données personnelles est contraint de respecter.

- **Collecte et traitement des données**

Entreprises, administrations et associations sont tenues d'informer les individus concernés de la collecte et du traitement de leurs données personnelles, et obtenir leur consentement en ce sens. Ces dernières ne seront récoltées que dans la mesure où elles sont nécessaires, et traitées uniquement à des fins spécifiques et légitimes.

- **Protection des informations**

Ces organismes doivent aussi mettre en place des mesures techniques et organisationnelles appropriées pour garantir la confidentialité et la sécurité des datas, telles que l'anonymisation, le chiffrement des informations (illisibles sans une clé d'autorisation), la gestion des accès, la destruction…

- **Transparence**

Le RGPD impose également à ces entités une totale transparence dans la manière dont les données seront traitées. Cela passe par la tenue d'un registre dédié (lire l'encadré ci-contre) et par la possibilité, pour les personnes concernées, de contacter un délégué à la protection des données (DPO). Les sociétés qui

UN REGISTRE, POUR QUOI FAIRE ?

Afin d'être en conformité avec le RGPD, les entreprises doivent créer un registre des activités de traitement des données. Sous forme de cahier ou de fichier numérique, par exemple, ce dernier contiendra, outre les informations personnelles (identités, adresses, téléphones…), un certain nombre de renseignements tels que les coordonnées du délégué à la protection des données (DPO), les finalités de leur traitement (concours, abonnement…), le délai prévu pour leur effacement ou encore la description des mesures techniques et organisationnelles mises en place pour les sécuriser.

Tous les citoyens et les résidents de l'Union européenne ont le droit à la protection de leurs données personnelles.

ne respectent pas les exigences du RGPD peuvent faire l'objet d'amendes élevées, jusqu'à 20 millions d'euros ou 4% de leur chiffre d'affaires mondial.

UNE NOTION QUI S'IMPOSE

Les données personnelles ont pris de l'importance au fur et à mesure de l'essor des nouvelles technologies et d'Internet. Elles font référence à toute information concernant une personne physique identifiée ou identifiable, comme son nom, son adresse ou son numéro de téléphone. L'expression «données personnelles» en elle-même apparaît à la fin des années 1940, plus précisément en 1949, quand le Conseil de l'Europe envisage pour la première fois de protéger la vie privée de ses citoyens. Une telle prise en compte résulte de la Seconde Guerre mondiale, où l'usage d'informations relatives à des personnes par des militaires ou des politiques – la constitution de listes de Juifs par les nazis, notamment – a dramatiquement illustré la nécessité d'un cadre juridique dans ce domaine. En 1970, le développement des technologies de l'information et de la communication accélère la réflexion. À l'époque, les gouvernements et les entreprises commencent à collecter et stocker >>

LA GESTION DES DONNÉES AUX ÉTATS-UNIS

En Amérique, il n'y a pas de loi fédérale sur la protection des données personnelles. Cependant, certaines industries ont établi leur propre réglementation (notamment dans le secteur de la santé) et des États ont voté des textes similaires à notre RGPD, comme la Californie ou le Colorado. Ailleurs, on se réfère à des règlements locaux sur la protection des consommateurs, car les Américains n'aiment pas voir les pouvoirs publics intervenir dans leur vie privée, même si c'est pour la protéger… Plusieurs lois ont été votées en ce sens, tels l'Electronic Communications Privacy Act (ECPA, restrictions sur les écoutes téléphoniques par le gouvernement, 1986), le Privacy Protection Act (protection des journalistes, 1980) et le Right to Financial Privacy Act (confidentialité des fichiers financiers personnels, 1978).

GOODPICS/ADOBE STOCK

>> de grandes quantités d'informations personnelles, alors qu'il n'existe pas encore de réglementation en la matière et que les individus concernés ne sont pas conscients de leurs droits.

DES GÉANTS DU WEB SANCTIONNÉS

Avec le temps, protéger la vie privée de tout un chacun devient une préoccupation majeure, ce qui conduit à la création de lois et de réglementations spécifiques. En 1995, la directive européenne 95/46/CE sur la protection des données à caractère personnel des citoyens de l'Union européenne (UE) est adoptée. Elle sera remplacée, en 2018, par le Règlement général sur la protection des données (RGPD), considéré comme l'un des textes les plus stricts sur le sujet. En 2022, les commissions informatique et libertés des États membres de l'UE ont sanctionné, à hauteur de 800 millions d'euros, les entreprises ne le respectant pas (le site Enforcementtracker.com permet de connaître en temps réel leurs décisions). En décembre 2022, Bing, la filiale européenne de Microsoft, a ainsi été sommée de payer 60 millions d'euros d'amende à cause de sa mauvaise gestion des cookies (dépôts pour de la publicité ciblée sans consentement, et problème d'équilibre entre les modalités d'acceptation et de refus). Ce même mois, Apple a écopé de 8 millions d'euros d'amende. Le géant américain n'avait pas recueilli le consentement des détenteurs français d'iPhone avant de se servir de leurs identifiants à des fins publicitaires… Auparavant, l'UFC-Que Choisir avait obtenu la condamnation de Google par le tribunal de grande instance de Paris, en 2019, pour la rédaction de 209 clauses abusives et illicites dans ses conditions d'utilisation et ses règles de confidentialité.

On notera que la notion de données personnelles évolue au fil des années, mais aussi au fur et à mesure des avancées technologiques qui permettent 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 continuer à protéger au mieux les individus. ■

À ADRESSER À UN ADMINISTRATEUR DE SITE POUR SE FAIRE DÉRÉFÉRENCER

Madame, Monsieur,

Des informations me concernant sont actuellement diffusées sur votre site internet, sur les pages suivantes : **[adresse web du site]**

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 que ces informations 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

Toute personne peut invoquer son droit à l'oubli (lire ci-contre). Voici une lettre-type pour l'exercer.

QUEL DROIT À L'OUBLI ?

Les moteurs de recherche peuvent devenir des alliés dans la reprise de contrôle sur vos données. Des requêtes, baptisées dorks, sont capables d'extraire celles cachées dans les profondeurs de la Toile… Mode d'emploi en cinq étapes.

Une méthode vous permet de vérifier si votre adresse électronique a été sauvegardée dans un espace numérique. Commencez par demander à un moteur de recherche – Google, par exemple – de détecter tous les fichiers texte (.txt) référencés dans ses bases de données. Pour ce faire, tapez le code suivant dans le cadre de recherche: «inurl:.txt». Cette commande, ou dork, peut se traduire de la sorte: «Google, peux-tu trouver, dans toutes les URL (adresses web) que tu as en mémoire, celles finissant par .txt?» C'est néanmoins un peu trop large, car le moteur affichera toutes les plateformes proposant un document en .txt: les réponses ne seront donc pas précises. Afin d'affiner votre requête, ajoutez à cette commande l'objet sur lequel porte la vérification, soit ici votre adresse électronique. La demande s'écrira alors ainsi: «inurl:.txt votre@mail.fr». Rappelons qu'il est possible de remplacer «votre@mail.fr» par n'importe quel autre type de fichier (Word, PDF, etc.) ou d'intitulé. Des pirates utilisent d'ailleurs cette technique pour faire ressortir les identifiants de connexion et les adresses électroniques enregistrés dans le serveur d'un site internet…

Conservez une copie de toutes les démarches effectuées.

1 CONTACTEZ LES ADMINISTRATEURS

Une fois que vous avez repéré les espaces numériques qui stockent indûment votre adresse e-mail, il faudra contacter leurs administrateurs… en espérant qu'ils vous répondent (et que ce ne soient pas des blogs abandonnés, par exemple). Car une erreur commise doit obligatoirement être corrigée. Premier point, leur rappeler les obligations 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 ensuite 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 des moteurs de recherche, ou du silence de webmasters de sites ayant sauvegardé >>

NE2PI/ADOBE STOCK

Un contenu effacé sur un moteur de recherche ne sera pas forcément déréférencé d'Internet.

>> 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 ACTIVEZ VOTRE DROIT À L'OUBLI

Qu'ils se nomment Google, Bing (Microsoft), Yahoo!, Archive, YouTube ou encore Qwant, ces sites ne peuvent pas faire tout ce qu'ils veulent. Fort heureusement, la loi est du côté des internautes. Depuis 2014, la Cour de justice de l'Union européenne a renforcé leur protection face aux informations diffusées par les moteurs de recherche. Ainsi, les Européens ont le droit de leur demander d'effacer les résultats proposés qui comportent leur nom (lire p. 15), si ces derniers sont «*inappropriés, inexacts, périmés, non pertinents ou excessifs*». Les acteurs du référencement ont un mois pour répondre. Attention, quand le renvoi sur le lien incriminé disparaît d'un moteur, le document en lui-même (ou la page) reste encore accessible sur Internet (lire ci-dessous)…

4 SUPPRIMEZ VOS DONNÉES DU WEB

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 de Yahoo! ou autre moteur de recherche ne suffit pas à sa suppression effective du Web. Pour que le contenu soit réellement éliminé et ne réapparaisse pas dans de nouveaux référencements, il faut contacter directement l'administrateur du site en question. Un e-mail est, certes, plus rapide, mais mieux vaut envoyer un courrier postal en recommandé (exemple de lettre-type p. 12).

5 VÉRIFIEZ SUR LE SITE ARCHIVE.ORG

Internet Archive (IA) 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 revenir en arrière», en français), elle regroupe d'autres types de supports tels que des logiciels, des images, des livres, des fichiers audio, des vidéos, etc. Les informations erronées vous concernant peuvent y être enregistrées. Afin de les faire effacer, envoyez un courriel à info@archive.org, avec l'URL du domaine litigieux et la raison pour laquelle vous désirez que la sauvegarde soit supprimée. Les administrateurs du portail Archive.org peuvent, dans certains cas, vous demander de confirmer la propriété du site référencé et stocké sur Wayback Machine; il vous faudra alors faire appel au webmaster. ■

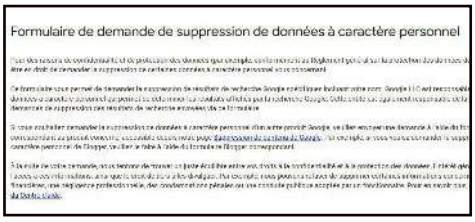
(1) Cnil.fr/fr/plainte/internet.
(2) Cnil.fr/fr/le-dereferencement-dun-contenu-dans-un-moteur-de-recherche.

NATABENE/ISTOCK

Fiches pratiques

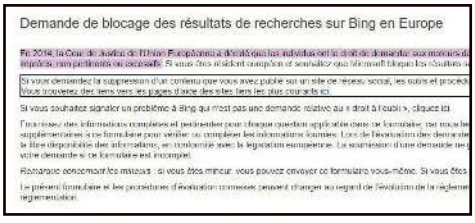
SUPPRIMER UN CONTENU

À chaque site sa méthode d'effacement… Présentation pour six d'entre eux.


Formulaire de demande de suppression de données à caractère personnel

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 (l'adresse) incriminée et votre identité (pour éviter les fausses demandes)


Demande de blocage des résultats de recherches sur Bing en Europe

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


Formulaire de demande de déréférencement

Qwant

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


Demandes de Blocage des résultats de recherche dans Yahoo Search :ressources pour les Résidents Européens

La Cour de justice de l'Union européenne a décidé que les **résidents européens** peuvent demander la désindexation d'adresses URL spécifiques figurant dans les résultats de recherches, portant sur leur nom et aboutissant à des pages contenant des informations personnelles **inexactes, inadéquates, qui ne sont plus pertinentes**, ou **excessives par rapport aux objectifs pour lesquelles elles ont été collectées ou traitées**.Les utilisateurs de Yahoo qui sont résidents européens peuvent utiliser ce formulaire afin de demander le blocage d'une URL pour une page associée à leur nom et qui répond à ces critères.Veuillez noter que tout blocage sera administré exclusivement pour la recherche du nom de la personne concernée.

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

Copains d'avant

1 Connectez-vous à votre compte et cliquez sur « Régler 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 »

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.

DANS LA TÊTE D'UN SMARTPHONE

Savez-vous ce que fait un téléphone avec vos données personnelles ? Découvrez-le à la lecture de cette journée type avec le « meilleur ennemi » de votre vie privée…

En 12 heures, votre smartphone peut envoyer, sur des serveurs distants, plusieurs millions d'informations. Cela va du code IMEI (pour International Mobile Equipment Identity, code relatif à l'«identité internationale d'équipement mobile», en français) de l'appareil à sa géolocalisation en passant par votre numéro de téléphone ou celui de votre carte SIM. En 2021, une étude menée par Doug Leith, chercheur en sécurité informatique à l'université de Dublin (Irlande), révélait une inquiétante collecte: toutes les 4 minutes 30 secondes, des dizaines de données personnelles sont transférées à des entreprises (constructeurs, opérateurs de téléphonie…) sans que nous en ayons conscience. Illustration.

LE MATIN

À peine réveillé, j'allume mon mobile: première connexion avec le fournisseur de services de communication. L'appareil établit immédiatement une liaison avec ma montre connectée, qui lui transmet des renseignements sur la nuit que j'ai passée. À première vue, tout va bien. Elle lui «explique» que mon sommeil profond a été bon; que j'ai rêvé à 3 heures du matin et que mon rythme cardiaque est satisfaisant.

Au même moment, toutes mes applications se mettent à jour; elles vont chercher de l'information. Les actualités du matin défilent selon ce que l'algorithme du téléphone a perçu de moi. Comme ce dernier connaît ma date de naissance (je la lui ai fournie lors de sa mise en route), il m'annonce aussi mon horoscope. J'ai Jupiter en Verseau, m'apprend-il, avant de me proposer une consultation payante chez une voyante (publicité ciblée). Grâce à la géolocalisation, l'heure et la météo locales apparaissent automatiquement. Mon smartphone m'indique également le trafic routier entre mon domicile et mon travail. Vu les bouchons, il me suggère de partir plus tôt. Et me rappelle, via une appli dédiée (Uber Eats, par exemple), que je dois faire des courses et qu'il n'y aura plus de lait demain dans le frigo si je ne clique pas sur le bouton «Acheter». Puis je surfe sur les réseaux sociaux (Instagram, Facebook…). Des contacts me saluent; ils ont repéré ma présence. Des robots analysent ce que j'aime lire et regarder, et me présentent des contenus en rapport.

Aujourd'hui, je suis obligé d'aller en voiture à mon bureau. Une fois installé au volant, je lance mon appli routière (GPS), sans oublier d'activer le Bluetooth pour que les enceintes du véhicule diffusent les messages. Je suis parti à l'heure conseillée par mon téléphone et heureusement, car il me signale un accident à cinq minutes de chez moi !

Géolocalisé dans le métro

D'habitude, je prends les transports en commun. Dans ce cas, je lance le NFC (système d'échange de données entre deux interfaces) de mon smartphone afin de profiter des options de paiement et d'identification sans contact du transporteur (la RATP, par exemple). J'achète des tickets dématérialisés via son application et je franchis les tourniquets du métro en badgeant avec mon portable. Ayant du mal à capter le réseau de mon opérateur à 20 mètres sous terre, je me connecte au wifi gratuit de la RATP – qui connaît, du coup,

Un smartphone peut envoyer, sur des serveurs distants, plusieurs millions de données en une demi-journée.

ALEXANDER/ADOBE STOCK

mon numéro de téléphone, le nom de mon appareil, ma géolocalisation, etc. Hier, un copain m'a interpellé: *«Ça va, Damien?»* Il a vu que j'étais dans la même rame que lui quand son smartphone a affiché «Wifi Téléphone Damien»!

DANS LA JOURNÉE

À la pause déjeuner, je passe devant une boutique. Mon mobile vibre aussitôt: certaines applications m'envoient en temps réel les offres promotionnelles de magasins croisés sur mon chemin. Là, je suis invité à acheter 15 litres de Coca-cola – dont je n'ai nul besoin, mais puisque c'est en promo… Un peu plus tard, je demande à mon moteur de recherche embarqué (Siri ou Google) de mettre ma chanson préférée dans mon casque connecté en Bluetooth. Je laisse le NFC ouvert; mon logiciel de musique sélectionne ensuite d'autres titres selon mes goûts. De telles applis (par exemple, Deezer, Spotify ou YouTube Music) sont aussi capables «d'entendre» l'environnement sonore autour de moi et de me proposer des morceaux en fonction.

Code IMEI transmis

Dans l'après-midi, je me connecte à des sites qui réclament la double authentification (2FA): je reçois un SMS afin d'accéder au portail web que je souhaite visiter. En échange, je dois donner mon numéro de téléphone. Dans certains cas (pour l'appli de ma banque, notamment), c'est l'identifiant unique de mon smartphone, le code IMEI, qui est transmis lors de ma connexion (il suffit de taper *#06# sur le clavier si on veut le connaître).

EN SOIRÉE

De retour chez moi, je programme plusieurs SMS à envoyer le lendemain matin. Puis j'allume la télévision via l'application mobile dédiée, proposée gratuitement par l'opérateur. Je ne passe plus par la TNT, mais directement par la box de mon fournisseur d'accès à Internet, qui sélectionne mes émissions préférées et affiche des offres vidéo en lien. Pas de chance, ce soir, sur les cinq films choisis par la box, trois sont payants! Je clique sur «Acheter» pour en voir un – inutile d'entrer mon numéro de carte bancaire, la machine l'a déjà en mémoire. Je n'ai qu'à valider mon achat.

Une publicité ciblée avant de dormir

Avant de me coucher, je me lave les dents avec une brosse connectée. Mon smartphone affiche celles que j'ai mal nettoyées. Au lit, tandis que je m'apprête à couper mon téléphone, ce dernier me signale qu'une mise à jour comportant des correctifs de sécurité doit avoir lieu. Il m'est recommandé de l'installer pendant la nuit, sinon mes données risquent d'être accessibles aux pirates… Je laisse donc mon portable branché. Alors que je m'endors, je reçois un dernier SMS. Une pub du constructeur me propose de changer d'appareil pour un neuf à moitié prix, à condition de renvoyer mon ancien mobile. Je n'ose pas le faire, j'ai toutes mes données, mes photos, mes vidéos, mes courriels et mes SMS sur celui-ci, et je ne sais pas comment les transférer ni les détruire… ■

PROTÉGER LES ENFANTS

Le RGPD a pour but de protéger les informations personnelles des citoyens. Mais qu'en est-il pour les mineurs, dont les données sont fortement convoitées ? Bénéficient-ils d'une protection spécifique ?

Le règlement général sur la protection des données (RGPD) au sein de l'Union européenne (UE) précise que les enfants de moins de 16 ans ne peuvent pas consentir au traitement de leurs informations personnelles, sauf si c'est permis par la loi nationale applicable (certains pays ont, en effet, fixé à 13 ans l'âge minimal pour donner son accord). Dans tous les cas, les parents ou les tuteurs légaux ont le droit d'autoriser cette opération au nom du mineur.

Selon le RGPD toujours, les entreprises, administrations ou associations qui collectent des datas sur des jeunes de moins de 18 ans ont l'obligation de prendre des dispositions particulières afin de garantir leur sécurité et leur confidentialité. Cela inclut des mesures techniques et organisationnelles appropriées, ainsi qu'une stricte limitation de la récolte de données à celles nécessaires aux finalités annoncées. Parents et enfants doivent aussi être informés de leurs droits et avoir la possibilité d'accéder simplement à leurs informations personnelles, afin de les contrôler, de les rectifier ou de les effacer. Des procédures pour gérer ces demandes et les traiter efficacement sont tenues d'exister.

Les réseaux sociaux sont concernés

Les règles à respecter en la matière ne s'appliquent pas uniquement aux structures situées dans l'UE, mais à toutes celles qui utilisent des données personnelles de citoyens de l'UE, qu'elles soient installées à l'intérieur ou à l'extérieur de l'Europe. Les réseaux sociaux n'en sont donc pas exempts

Seuls les jeunes de plus de 15 ans peuvent consentir au traitement de leurs données personnelles.

IMGORTHAND/ISTOCK

CAR'ADO, UN OUTIL DÉDIÉ À LA PRÉVENTION

Dans le Nord de la France, la gendarmerie nationale a créé Car'Ado, une caravane destinée à sensibiliser les adolescents sur différents thèmes. Une centaine de jeunes volontaires y partagent des conseils avec d'autres camarades. Sujets abordés ? Violences, sexisme, cyberharcèlement… Car'Ado se déplace lors de salons, sur les plages ou dans les lycées. Plus d'informations sur **Gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/dans-le-nord-a-bord-de-la-car-ado.**

GEND/SIRPA/A. FAURE

et contraints de mettre en place des mesures spécifiques, telles qu'un âge minimal pour l'inscription, des politiques de confidentialité et de protection des données adaptées aux enfants, ainsi que des efforts pour prévenir la désinformation, le harcèlement et les contenus inappropriés.

Au Canada et aux États-Unis, des supports vidéo ludiques ont été montrés du doigt pour laxisme avéré. Epic Games, par exemple, s'est vu infliger une amende de plus de 453 millions d'euros à la suite de deux plaintes du régulateur américain de la concurrence, la Federal Trade Commission (FTC). Cet éditeur de jeux vidéo a été accusé d'avoir violé la loi sur la protection de la vie privée des enfants en ligne (COPPA), car ces derniers pouvaient participer à des tchats vocaux dans Fortnite et Rocket League sans que les parents n'aient été invités à valider l'inscription en ligne.

Les adolescents, des cibles de choix

Vérifier l'âge d'une personne qui crée un compte sur les réseaux sociaux est obligatoire, ce qui n'empêche pas les mineurs de s'inscrire sans trop grande difficulté: selon Audirep, un institut d'études marketing, 81 % des 8-18 ans possédaient un compte Snapchat en 2021, et 69 %, un compte Instagram… le tout sans que leurs parents soient forcément au courant. Des mesures plus ciblées ont par conséquent été adoptées afin de mieux protéger les adolescents. Par exemple, si les 13-14 ans peuvent se créer un profil sur un réseau social, ce dernier doit avoir reçu, pour activer leur compte, le consentement des jeunes concernés comme celui de leurs parents. Ceux qui sont âgés de 15 ans, quant à eux, ont le droit de s'inscrire seuls, car ils sont considérés comme majeurs sur les réseaux sociaux.

La mise en place de *safe zones* («zones sécurisées», en français) constitue un autre aspect de la protection des mineurs. L'opérateur Orange, notamment, a installé, en novembre 2022, de telles zones dans Fortnite, Roblox et Minecraft, trois des jeux vidéo particulièrement plébiscités des enfants. Ces espaces en ligne sont destinés à répondre aux questions des plus jeunes sur les jeux immersifs et à collecter les plaintes de victimes ou de témoins de cyberharcèlement. Il suffit au joueur de faire bondir son personnage sur un gros bouton baptisé «Jump to talk» pour lancer une alerte de cyberharcèlement à un robot. Celui-ci prodigue alors des conseils et propose d'appeler le 3018: gratuit, anonyme et confidentiel, ce numéro national est dédié à ceux qui subissent des violences numériques. ■

SOMMAIRE

L'identité numérique

Acquérir les bons gestes numériques est un apprentissage de chaque jour. Il est essentiel, car seule une « hygiène » adaptée – utilisation réfléchie des mots de passe, gestion éclairée de son identité 2.0, partage sécurisé d'informations sensibles… – permet de protéger ses données personnelles et sa vie privée.

Parce que les pirates du Web n'attendent qu'une chose, c'est de pouvoir s'en emparer ! Selon une étude publiée en février 2023 par la société Adastra, 77 % des décideurs informatiques des États-Unis et du Canada pensent que leurs entreprises seront probablement confrontées à une violation de leurs données durant les trois prochaines années… De son côté, la société BlackBerry a dénombré 1757 248 cyberattaques entre le 1er septembre et le 30 novembre 2022. Leur objectif ? Voler des informations personnelles. Ce chapitre tente donc de vous aider à construire, pas à pas, votre propre couteau suisse de cybersécurité.

TETE_ESCAPE/ADOBE STOCK

SÉCURISER SON IDENTITÉ : LES TROIS RÈGLES D'OR

Pour rester serein sur Internet, on a tout intérêt à mettre en place des mesures de protection. Présentation des trois plus importantes.

1 Avoir un mot de passe solide, c'est la base

Se créer une identité numérique fiable et sécurisée n'a rien de compliqué. Il suffit de suivre quelques règles simples et d'employer des outils adaptés. Au départ, on choisit un nom d'utilisateur et un mot de passe solides. Le premier doit être unique et dur à deviner; le second, complexe dans sa dénomination et difficile à pirater – pour cela, rien de tel qu'une combinaison de lettres, de chiffres et de symboles. Par ailleurs, il convient de se doter d'une adresse mail et d'un mot de passe unique par site, forum, logiciel, etc. C'est indispensable. Ainsi, si une fuite de données a lieu, les autres accès ne sont pas mis en danger. De nombreux sites génèrent gratuitement des mots de passe sécurisés – parmi eux, ceux de la Cnil[1] et de 1Password[2] sont recommandés (jamais de mot de passe avec uniquement des lettres). Installer un antivirus sur son ordinateur et recourir à un service de gestion de mots de passe pour les conserver en toute sécurité constituent deux autres bonnes pratiques.

2 Opter pour la double authentification

La double authentification, ou 2FA, ajoute une couche de protection. Elle doit faire partie du quotidien de tout consommateur. Une boutique ou un site la propose? On les choisira en priorité, en particulier pour des achats en ligne. Comment ça marche? En général, pour s'identifier sur un site sécurisé par la 2FA, on doit fournir un code à usage unique et limité dans le temps en plus du traditionnel duo identifiant (adresse mail/numéro de téléphone) et mot de passe. La méthode la plus sûre à ce jour est celle qui recourt à une application d'authentification téléchargée sur smartphone (Google Authenticator[3], Microsoft Authenticator[4], Authy by Twilio[5], etc.). Pour mettre en place un accès sécurisé la première fois, on scanne, avec l'appli d'authentification, un QR Code envoyé par le site sur lequel on a un compte. Ce dernier est ainsi lié à l'application, laquelle générera ensuite des codes uniques valables quelques secondes à chaque connexion. La vérification en deux étapes peut se faire d'autres manières, par exemple par e-mail, SMS ou appel téléphonique automatisé. Il est fortement conseillé de doubler cette seconde vérification: application + courriel, ou courriel + SMS. Attention, s'il existe plus de 60 outils dédiés à la 2FA, certains sont destinés à un seul service – c'est le cas, par exemple, chez les éditeurs de jeux vidéo (Ubisoft, Steam, etc.). Prudence ici: si le mot de

RESTER VIGILANT

Tout internaute a intérêt à apprendre à reconnaître les courriels de phishing et les sites web suspects. Les indices qui doivent alerter : un logo ressemblant fortement à celui d'une marque connue, une adresse électronique de contact ne comportant pas le nom de domaine du site web concerné, une absence d'adresse physique en France… Règles de sécurité de base : ne jamais ouvrir les liens ou les pièces jointes provenant de sources douteuses, ni donner ses informations de connexion à des tiers.

F. PRINCIPE/ADOBE STOCK

passe est perdu, que le téléphone est cassé ou que l'appli est effacée par mégarde, il n'y a plus d'accès possible à l'espace protégé par la 2FA ! Il faudra des démarches longues et fastidieuses auprès du site pour le convaincre de le rouvrir.

3 Utiliser un VPN, si l'on est en déplacement

Pour les grands voyageurs, les réseaux privés virtuels (VPN) constituent une bonne solution de protection. Il en existe des dizaines sur le marché (VyprVPN [6], Proton VPN [7], etc.). Attention, ceux rendus les plus «visibles» par la publicité ne sont pas forcément les meilleurs ! Pour rappel, un VPN masque l'adresse IP [8] de l'utilisateur puis chiffre le trafic internet entre ce dernier et ce qu'il visite (boîte électronique, forum, site, etc.). Le but: rendre ces allers-retours impénétrables pour les escrocs qui les intercepteraient, et l'internaute plus difficile à suivre pour des tiers (sites web, pirates, etc.). Rappelons toutefois que passer par un VPN ne signifie pas rester anonyme, loin de là: les fournisseurs de ces réseaux virtuels connaissent leurs clients, car ces derniers leur livrent des informations personnelles pour se connecter… Bref, dans tous les cas, dès que l'on est amené à partager certaines données, il faut s'assurer de le faire de manière sécurisée. ■

PAS-À-PAS
Surfez sans risque

- **Créez-vous une adresse électronique personnalisée** par secteur d'activité (administration, école, commerce, etc.).
- **Déterminez un mot de passe sécurisé de 15 caractères** au minimum. Il doit contenir des lettres, majuscules et minuscules, des chiffres et des signes de ponctuation.
- **Sélectionnez la double authentification** (2FA), qui fonctionne sur le principe d'une double clé d'accès.
- **Optez pour un VPN lorsque vous êtes en déplacement.** Cela permet d'empêcher tout suivi de votre activité en ligne et toute interception de message.

(1) Cnil.fr/fr/generer-un-mot-de-passe-solide. (2) 1password.com/fr/password-generator. (3) Disponible sur Google Play et l'App Store. (4) Microsoft.com/fr-fr/security/mobile-authenticator-app. (5) Twilio.com/fr/authy. (6) Vyprvpn.com. (7) Protonvpn.com. (8) Une adresse IP (Internet Protocol Address) *est une série de nombres uniques identifiant un appareil connecté (pour en savoir plus, lire aussi p. 34-35).*

LES ACTES DE PIRATAGE ONT EXPLOSÉ

Êtes-vous certain de protéger au mieux vos informations personnelles ? Nombreux sont ceux qui les convoitent ! Alors, suivez nos conseils pour vous prémunir des vols et des utilisations abusives de vos données.

Dans 23 % des cas, les fuites de données personnelles sont causées par une simple erreur humaine (source: IBM). Par ailleurs, une cyberattaque a lieu toutes les 39 secondes (source: université du Maryland, États-Unis). Enfin, une donnée volée sera utilisée près d'une centaine de fois en moins de cinq minutes (source: SVZ). Ces trois chiffres doivent mettre tous vos sens d'internaute en alerte, et vous inciter à mettre en place sans tarder une protection efficace des informations permettant de vous identifier (nom, adresse, numéro de téléphone… mais aussi emploi, état civil, origine ethnique, préférence politique ou religieuse, etc.). Si elles tombent entre les mains de personnes mal intentionnées, ces datas peuvent servir à du spamming (envoi de courriels non sollicités, de publicités, etc.) ou, pis, à des arnaques en ligne (hameçonnage, piratage de compte, fausse vente, etc.).

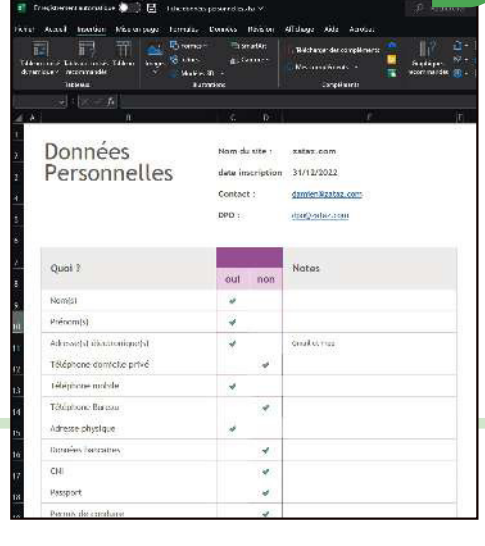
Les lois sur la protection de la vie privée varient selon les pays, mais elles visent en général à protéger les citoyens contre l'emploi abusif de leurs données personnelles. Régulièrement, ces législations se durcissent; il faut dire que les piratages ont explosé ces dernières années. Pour preuve, le site Cybermalveillance.gouv.fr observait une hausse de 400 % entre mars 2020 et mars 2021 ! Selon Reed Smith, un cabinet d'avocats international, la pandémie de Covid-19 a d'ailleurs été la période où la sécurité numérique a été la plus menacée.

Être identifié, c'est devenir 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. Cette dernière doit en conserver la maîtrise. Si ce n'est pas le cas, et qu'elle se fait dérober ses données, elle

GÉREZ VOS INSCRIPTIONS

Créez un tableau (sur papier, tableur Excel, etc.) pour regrouper toutes les informations que vous divulguez lors de vos inscriptions sur des sites internet. Ainsi, en cas de besoin, vous saurez qui a quoi et, surtout, qui contacter pour faire valoir vos droits. Nous vous conseillons d'y inclure les adresses électroniques des responsables du traitement des données personnelles (DPO) des portails web auxquels vous avez affaire.



Les internautes utilisent souvent des mots de passe trop simples, afin de ne pas les oublier. La Cnil propose un outil en ligne pour remédier à ce problème.

RESSOURCES BIBLIOGRAPHIQUES

- **IBM** Ibm.com/security/data-breach *(en anglais)*
- **Université du Maryland** Eng.umd.edu/news/story/study-hackers-attack-every-39-seconds *(en anglais)*
- **SVZ** Veillezataz.com/post/fuite-de-donn%C3%A9es-plus-de-90-acc%C3%A8s-en-moins-de-5-minutes
- **Reed Smith** Reedsmith.com/en/perspectives/2020/03/coronavirus-is-now-possibly-the-largest-ever-security-threat *(en anglais)*
- **Cnil** Cnil.fr/fr/definition/donnee-personnelle

peut se retrouver identifiée directement (via son nom et son prénom), indirectement (par son téléphone ou sa plaque d'immatriculation, son numéro de Sécurité sociale, son adresse postale ou e-mail… mais aussi sa voix ou son image !), ou encore par croisement (par exemple: date de naissance + adresse postale + nom de famille). Bref, dès qu'il est identifié, l'internaute peut devenir la cible de cyberattaques.

Les bonnes pratiques, ça doit devenir automatique !

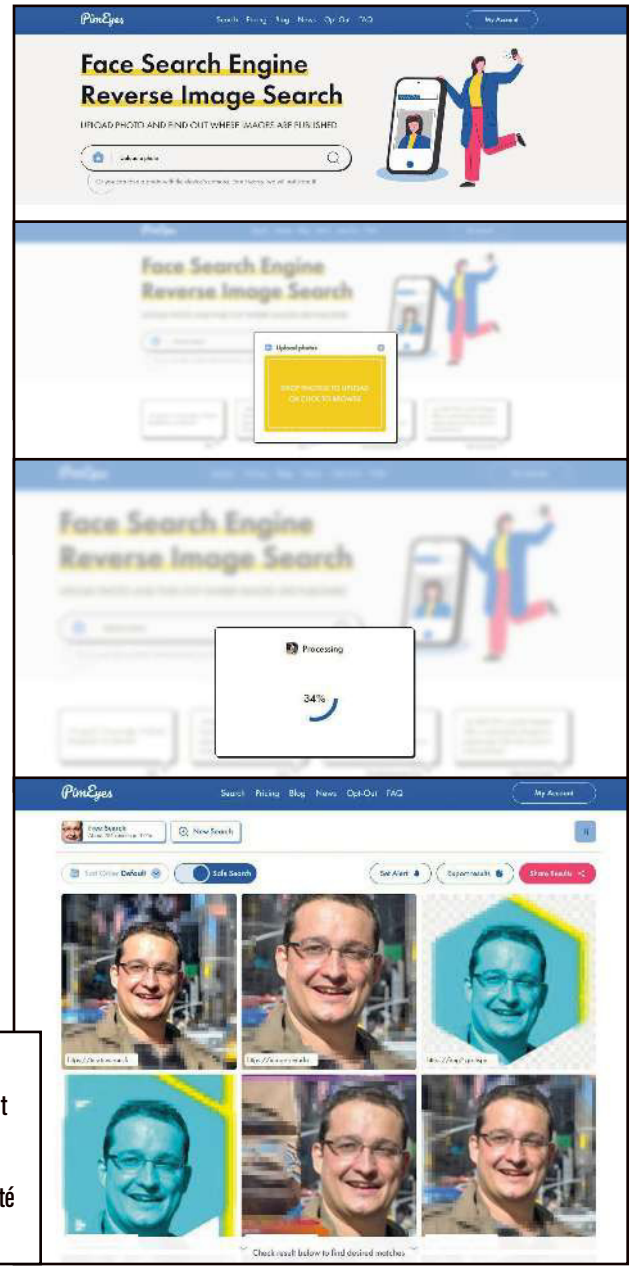
Pour les éviter, il existe plusieurs choses à faire, les plus simples étant souvent les meilleures. Hélas, ces bonnes pratiques ne sont pas encore mises en œuvre par tous. Alors martelons-les: il faut se doter d'un mot de passe fort et unique pour chaque compte en ligne; activer la double authentification (2FA) pour les comptes sensibles (lire p. 22); ne jamais cliquer sur des liens dans les messages suspects (75 % des vols d'informations ont lieu via ce vecteur); garder ses logiciels et ses appareils à jour, afin d'éviter les failles de sécurité; installer un antivirus pour protéger son équipement informatique et mobile; ne pas partager ses données personnelles sur les réseaux sociaux ou les sites non sécurisés; toujours se poser la question de l'utilité qu'il y a à fournir des informations à un site web (par exemple, *«Ai-je vraiment besoin de donner mon adresse postale alors que je ne me fais rien livrer ?»)*; passer par une connexion privée ou un réseau virtuel privé (VPN) si on utilise un réseau public (celui offert par votre restaurant favori, votre club de sport…); être vigilant lorsqu'on surfe sur des ordinateurs publics ou partagés (comme ceux proposés gratuitement dans les hôtels); savoir qui a accès à ses données et comment elles sont traitées (pour cela, il est recommandé de répertorier sites et organismes sur un tableau – lire aussi l'encadré «Gérez vos inscriptions», p. 24).

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 demander les informations qu'elle a fournies et la concernant au délégué à la protection des données (DPO) d'un site, de les réemployer et de les transmettre à un autre responsable (article 20 du Règlement général sur la protection des données). Lorsque l'entreprise ou l'organisme ne dispose d'aucune data sur le demandeur, le DPO doit tout de même lui répondre dans un délai d'un mois. ■

VOTRE PORTRAIT INDÛMENT EXPLOITÉ

Les fuites de données personnelles ne concernent pas que les numéros de Sécurité sociale ou les e-mails… La preuve par l'image.

Votre identité numérique passe également par votre image, notamment votre portrait. Et lui aussi peut être utilisé à votre insu. Imaginez: une photo de vous, tirée d'une de vos soirées, se retrouve dans la communication d'une boîte de nuit, reprise sur son site web, ses profils sociaux… Êtes-vous d'accord pour servir de panneau d'affichage publicitaire gratuit ? Voici quelques outils pour vous aider à dénicher les fautifs, à les contacter et à reprendre la main sur vos clichés.



PimEyes

Le site PimEyes, fondé par une société polonaise, est capable de repérer les espaces numériques employant indûment votre image. Efficace et redoutable, ce moteur de recherche particulier (Peameyes.com) trouve en quelques secondes, à partir de la photographie que vous lui soumettez, les adresses des sites qui l'utilisent, et vous indique les éventuelles modifications apportées au cliché (passé en noir et blanc, colorisé, etc.). Le tout gratuitement. Il référence actuellement plus de 900 millions de portraits sous forme de signatures biométriques – donc pas directement des visages. Son concurrent (non public), l'américain Clearview AI, en stockerait quant à lui plus de 3 milliards dans sa base de données… Les performances de PimEyes en

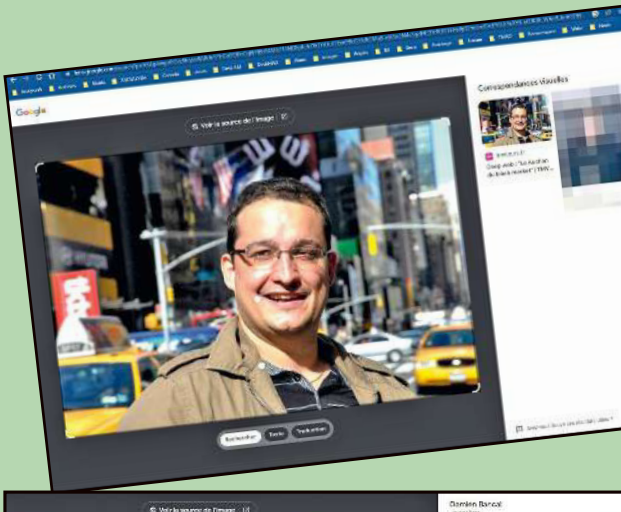
PimEyes permet de rechercher des photos de vous exploitées par d'autres internautes. Proposez votre portrait au moteur de recherche ; l'analyse terminée, il affichera votre photo et ceux qui l'exploitent. Il vous dira même si elle a été modifiée. Une version payante offre la possibilité d'explorer le deepweb (les profondeurs d'Internet).

Via Google Image, sélectionnez le petit appareil photo entre le micro et la loupe. Glissez votre photographie ; le moteur de recherche en affichera les concordances. Recadrez votre document afin d'affiner la pertinence des réponses.

reconnaissance faciale sont redoutables. En 2020, à la suite de la défaite du président américain Donald Trump, des dizaines d'internautes s'étaient servi de ce site pour tenter d'identifier les émeutiers du Capitole. C'est d'ailleurs son (gros) défaut: point n'est besoin de s'inscrire et/ou de s'authentifier pour l'utiliser… Résultat, n'importe qui peut trouver n'importe quoi à partir d'une photo qui ne lui appartient pas. À noter: une option payante existe pour rechercher des informations dans le deepweb, cet espace regroupant les sites internet accessibles mais non référencés.

Google Image

Google, via son moteur spécial images (Images.google.com), donne la possibilité d'effectuer une recherche sur un document photographique spécifique – à condition que le cliché soit référencé par les robots du géant américain. Le principe est simple: après avoir cliqué sur l'appareil photo accolé à la barre de recherche, vous proposez le visuel à analyser. En quelques secondes, Google Image affiche les concordances et les adresses web des utilisateurs de ladite illustration. Il est possible de recadrer la représentation afin d'éliminer, par exemple, des bâtiments, un meuble ou d'autres personnes qui perturberaient l'action de l'intelligence artificielle.



Forensically

En anglais et gratuit, ce site créé en 2015 par l'ingénieur informatique suisse Jonas Wagner (29a.ch/photo-forensics), propose des outils en ligne étonnants. Il ne vous dira pas où se trouve votre portrait, mais vous saurez si votre photographie, réutilisée par d'autres, a été modifiée, clonée, sujette à des ajouts d'objets, de décors… En bref, trafiquée. Un moyen de plus pour tenter de maîtriser sa vie numérique. ■

LE COURRIEL, NOTRE MEILLEUR ENNEMI

Le courrier électronique demeure, dans plus de 75 % des cas, la porte d'entrée des erreurs et des actes de malveillance en ligne. Voici nos recommandations pour limiter les risques.

Ne vous fiez pas aveuglément au nom de l'expéditeur d'un courriel reçu dans votre boîte personnelle. Soyez à l'affût de tout indice trahissant la véritable origine de votre correspondant, surtout si cet e-mail comporte des pièces jointes ou des liens. Par exemple, un message qui ne «colle» pas, dans la forme ou le contenu, à ce que votre interlocuteur légitime enverrait normalement: des fautes, des tournures de phrases bizarres, des sollicitations incongrues (*«J'ai perdu mon portefeuille, je suis coincé à l'étranger»; «J'ai quelque chose à te demander, mais il ne faut en parler à personne»*; etc.). En cas de doute, appelez votre contact et faites-vous confirmer qu'il est bien l'expéditeur, car même si l'adresse électronique est la sienne, il a pu se faire pirater sa messagerie… et avoir envoyé un message infecté à son insu.

ONEPHOTO/ADOBE STOCK

Pas d'informations personnelles par e-mail

Sachez que les organismes ou entreprises officiels ne vous demanderont jamais de donner par courrier électronique des renseignements confidentiels (numéro de Sécurité sociale, coordonnées bancaires, carte d'identité, etc.). Si c'est le cas, contactez l'expéditeur pour confirmation, car un tel e-mail peut cacher une tentative d'hameçonnage de vos données – le correspondant usurpant l'identité d'un tiers ou d'un site Internet en qui vous avez a priori confiance – opérateur téléphonique, banque, boutique, service des impôts, Assurance maladie… De même, les chaînes de lettres (partager un message pour rentrer dans le *Livre des records*), les porte-bonheur, les propositions financières (gagner de l'argent avec la cryptomonnaie), les appels à la solidarité ou encore les alertes aux virus dissimulent parfois des tentatives de tromperie. Évitez aussi de transférer de tels messages ou de mettre un avis sur les réseaux sociaux, même si vous connaissez l'expéditeur.

Des liens à vérifier avant de cliquer

Vous avez reçu un courriel vous invitant à visiter un site web: placez votre souris sur le lien indiqué – sans cliquer dessus ! – et regardez ce qui apparaît. Cela correspond-il à l'adresse URL du site ? Si ce n'est pas le cas, méfiez-vous ! Dans tous les cas, il >>

Astuces RÈGLES DE BASE POUR SÉCURISER SA MESSAGERIE

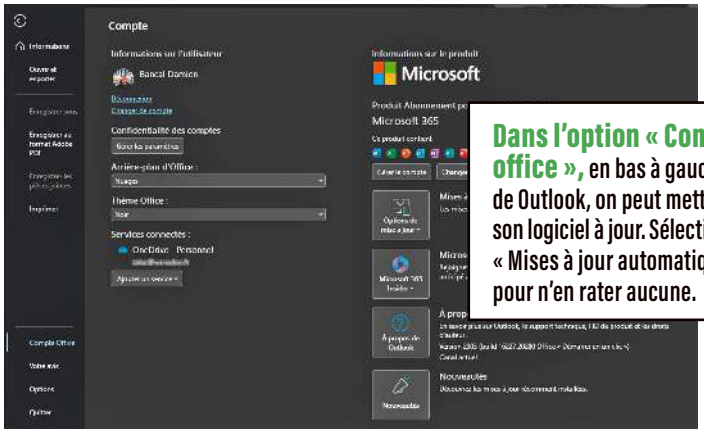
METTRE À JOUR SON LOGICIEL DE MESSAGERIE (Outlook, Thunderbird). Si possible, activer les mises à jour automatiques, les éventuelles vulnérabilités seront ainsi corrigées au fur et à mesure.

DÉSACTIVER L'APERÇU DES MESSAGES REÇUS en reconfigurant sa boîte. En effet, certains e-mails peuvent contenir du code infecté ; cela évitera de le lancer.

INTERDIRE L'EXÉCUTION D'OPTIONS, comme les contrôles ActiveX ou les plug-ins, afin d'empêcher la propagation de virus. Pour ce faire, modifier les paramètres de sécurité.

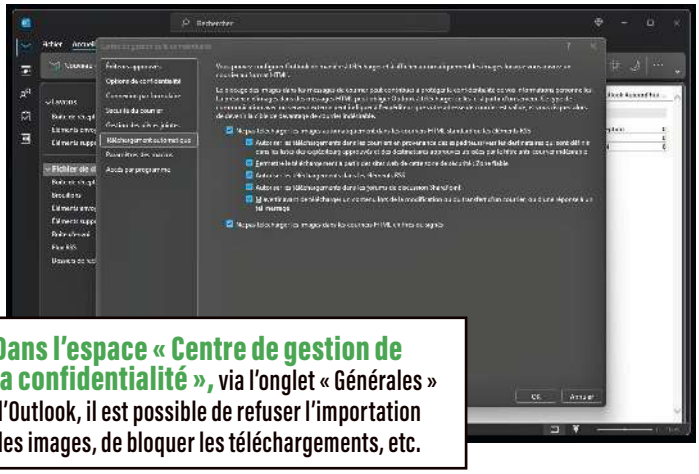
BLOQUER LES TÉLÉCHARGEMENTS AUTOMATIQUES et imposer une demande de permission de télécharger les pièces jointes. Cela limite les risques de se retrouver avec des logiciels malveillants sur son disque dur.

LIRE LES COURRIELS EN TEXTE BRUT de préférence. Il suffit pour cela de configurer sa messagerie en empêchant l'affichage des e-mails en HTML. De fait, ce format peut être utilisé par les pirates afin de dissimuler du code malveillant. ■



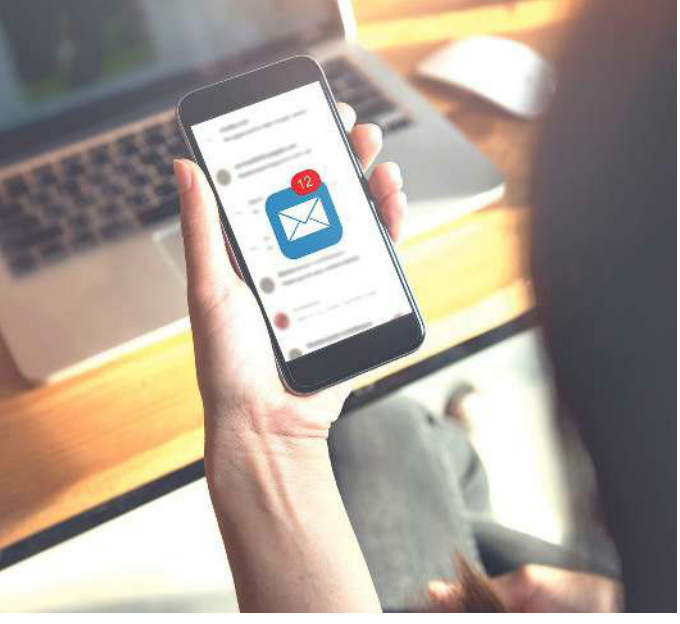
Dans l'option « Compte office », en bas à gauche de Outlook, on peut mettre son logiciel à jour. Sélectionner « Mises à jour automatiques » pour n'en rater aucune.

Dans l'option « Générales » d'Outlook, on choisit de recevoir ses courriels au format texte brut.



Dans l'espace « Centre de gestion de la confidentialité », via l'onglet « Générales » d'Outlook, il est possible de refuser l'importation des images, de bloquer les téléchargements, etc.

NOUN PROJECT



>> est préférable de saisir manuellement une adresse web dans un navigateur plutôt que de cliquer sur un lien. Lisez aussi attentivement le message. Remarquez s'il y a des caractères accentués (cyrillique, chinois, etc.) ou modifiés (le O n'est-il pas plutôt un 0 ?) et étudiez le niveau de langue française de votre interlocuteur. Dans la plupart des tentatives de phishing, surtout lorsqu'elles viennent de l'étranger et que le texte a été traduit par un logiciel, l'orthographe et la tournure des phrases sont mauvaises. Les caractères accentués sont parfois mal retranscrits. Cependant, les pirates se professionnalisant, aujourd'hui des mails frauduleux peuvent comporter exprès quelques fautes dissimulées dans le texte; les escrocs estiment en effet avoir plus de chances de piéger leurs cibles quand celles-ci n'ont pas prêté attention aux fautes !

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, il existe de nombreux portails web qui en créent d'éphémères. Si vous souhaitez, par exemple, faire une demande de devis en ligne, passez par Trash Mail. Ce site génère une adresse dont la durée de vie va d'un jour à un mois; ensuite, la redirection fantôme transfert le devis sollicité sur votre véritable boîte électronique, sans que cette adresse n'ait été fournie au correspondant. 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 ces deux cas, 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 spécialement dédié aux achats

Vous souhaitez utiliser votre adresse électronique pour vos achats en ligne, vos loisirs ou encore pour vos échanges avec l'administration. Mais alors, tous vos œufs sont dans le même panier numérique ! Pour éviter cette situation, il est fortement conseillé de créer des « alias », c'est-à-dire des adresses électroniques 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 comme SimpleLogin pour Proton Mail, ou encore Firefox Relay pour la fondation Mozilla, proposent gratuitement des outils pour créer des alias.

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 gratuit Hunter (« chasseur », en français) peut découvrir en quelques secondes à peine l'utilisateur d'une adresse e-mail professionnelle. L'objectif de Hunter.io/fr ? Vous donner le moyen de répondre rapidement à une question simple: *« Cette personne est-elle vraiment employée par l'entreprise qui me contacte ? »* ■

BIENTÔT LES VACANCES...

Petit rappel des mesures à prendre pour qu'un super séjour ne devienne pas un cauchemar au retour.

Dotez-vous d'une adresse mail spéciale vacances !

AVANT DE PARTIR

Pensez à créer une adresse électronique spéciale vacances, avec une signature codée pour vos correspondants; par exemple, un triple smiley souriant. Ainsi, sans ce signe distinctif, ils sauront que les mails ne viennent pas de vous. Mission de l'adresse mail éphémère: maintenir le contact avec la famille et les amis, mais aussi servir aux guides et hôtels locaux. Il est également utile de sauvegarder, sur une clé USB, les copies de vos pièces d'identité et les numéros de téléphone importants (ambassade, etc.), dans un fichier que vous protégez avec l'outil 7-Zip (logiciel de compression de données et d'archivage de fichiers). Vous pouvez également prévoir une pochette anti-NFC pour éviter la copie, en sans-fil, des informations de votre carte bancaire et de votre passeport. En partant, coupez le wifi de votre domicile et activez, si ce n'est pas déjà fait, la double authentification – avec une gestion par clé physique ou application plutôt que par SMS ou mail.

PENDANT LE SÉJOUR

Suivez la pièce d'identité que vous fournissez aux réceptions des hôtels. En cas de copie (papier ou numérique), il faut pouvoir demander à la contrôler, en y rajoutant un élément comme la date et le lieu (nom de l'hôtel, etc.). Par ailleurs, ne vous servez pas des ordinateurs proposés gratuitement dans les hébergements à des fins privées et/ou professionnelles. S'il n'est pas possible de faire autrement, il ne faudra pas oublier de détruire le fichier que vous avez utilisé – le mettre simplement à la poubelle ne suffit pas. Mode d'emploi pour une destruction sûre: créer un fichier du même nom que celui précédemment ouvert, le remplir d'images et de milliers de chiffres, écraser l'ancien document avec le nouveau. Ne pas hésiter à reproduire cette action plusieurs fois ! Si vous pensez avoir besoin, à un moment, d'imprimer quelque chose (un billet d'avion, par exemple), faites-en une copie sur votre clé USB en amont – c'est cette version que vous sortirez sur papier. En vacances, et d'autant plus hors de France, il faut éviter au maximum de se connecter à un site internet contenant ses données et de consulter ses courriels personnels et/ou professionnels. En tout cas, JAMAIS via un wifi public ! En voyage, passer par un réseau privé virtuel (VPN) s'avère plus sûr. Attention, certains pays les bloquent… Enfin, il n'est pas recommandé de mettre à jour son ordinateur, sa tablette, son téléphone et ses applications quand on se trouve à l'étranger.

AU RETOUR

Si vous n'avez pas pu faire autrement que de vous connecter à votre compte électronique ou à un site contenant vos données personnelles pendant votre séjour, changez immédiatement vos mots de passe une fois chez vous. Fermez l'adresse e-mail dédiée aux vacances (pas de réexploitation lors des prochaines). Enfin, mettez à jour ordinateur et objets connectés. ■

OATAWA/ADOBE STOCK ; PEOPLEIMAGES.COM/ADOBE STOCK

SURFER SANS SEMER SES INFOS AUX QUATRE VENTS

En naviguant sur la Toile, on laisse énormément de traces. Certaines volontairement, d'autres non. Comment surfer sans trop se dévoiler ?

On visite un site internet, on s'y inscrit. Effectuée par des milliers d'individus chaque jour, cette action déverse sur le web des montagnes de données personnelles. Celles apportées lors des inscriptions (nom, adresse électronique, téléphone, etc.), mais aussi celles que les internautes n'imaginent pas, comme leur géolocalisation, l'environnement système de leur ordinateur ou encore les informations sur le navigateur qu'ils utilisent. En la matière, il en existe une dizaine sur le marché, chacun avec ses propres fonctionnalités, ses différences et ses communautés.

Les plus connus sont Google Chrome, Mozilla Firefox, Apple Safari, Microsoft Edge, Opera, Waterfox, Comodo Dragon, Maxthon, Brave, Vivaldi et Torch Browser. Le premier est populaire pour sa rapidité et sa facilité d'utilisation. Il a été pensé pour s'intégrer avec d'autres produits Google, comme Gmail ou YouTube. Mozilla Firefox, lui, est apprécié pour sa vitesse et sa sécurité, ainsi que pour sa grande communauté de développeurs concevant régulièrement des extensions pour ajouter des options (analyse d'un site, traduction…). Safari est le navigateur par défaut des appareils Apple. Microsoft Edge est basé sur le même moteur de rendu que Google Chrome, mais offre des fonctionnalités supplémentaires, telles la lecture de livres numériques ou la navigation en mode lecteur. Opera, dernier du Top 5, dispose d'options uniques comme le VPN intégré.

1 Opter pour la navigation anonyme

L'option « navigation anonyme » est toujours proposée par le navigateur. Pour que des informations ne s'enregistrent pas dessus quand il surfe, l'utilisateur doit activer cette fonctionnalité. Attention, cela ne veut pas dire que les sites qu'il visitera ne capteront pas ses faits et gestes, mais simplement qu'ils auront moins de données à analyser. En effet, l'historique de navigation, les informations de formulaire, les cookies, etc., ne seront pas conservés; les mots de passe, les préférences sélectionnées (langue, couleur de lecture…) ne seront pas sauvegardées. La navigation anonyme est donc protectrice, mais elle ne garantit pas une confidentialité totale. Lorsqu'elle fonctionne, il devient juste plus difficile pour des tiers de suivre les activités en ligne de l'internaute. Mais, les informations le concernant peuvent encore être collectées par les sites web visités, les fournisseurs d'accès à internet, les gouvernements, etc.

LE SMARTPHONE : UN ORDI DANS LA POCHE

Les smartphones de dernière génération sont de véritables ordinateurs installés dans vos poches. Quand vous surfez, vous devez donc avoir la même hygiène numérique que sur votre ordinateur. Il faut, en plus, prendre en compte certaines spécificités de ces matériels nomades. Ainsi, coupez le wifi, le Bluetooth et le NFC* si vous n'en avez pas besoin. Ces outils de communication peuvent servir à de la collecte d'informations non autorisée.

**NFC pour Near Field Communication. Cette technologie de transmission sans fil, intégrée à de nombreux smartphones Android, fonctionne à courte portée et permet l'échange d'informations entre deux smartphones ou appareils compatibles.*

Activez la fonction « navigation anonyme » pour limiter le suivi et la conservation de vos données.

2 Protéger son navigateur avec un antivirus

Quel qu'il soit, un navigateur moderne offre une protection contre les logiciels malveillants, les pop-up indésirables et les sites frauduleux. Il n'en reste pas moins fragile face aux pirates, qui s'acharnent à traquer la moindre vulnérabilité pour accéder à des données. Dès lors, des mises à jour régulières du système d'exploitation de l'appareil et du navigateur web s'imposent, car elles corrigent généralement des failles de sécurité. Un antivirus est également bienvenu, mais attention: sans actualisation de sa base de données de signatures virales, il ne sert plus à grand-chose ! Il faut donc absolument cocher la « mise à jour automatique » sur cet outil.

3 Se servir des widgets

Nombre de navigateurs proposent des applications (widgets) pour faciliter et sécuriser les surfs. Certains peuvent géolocaliser l'emplacement d'un site web; d'autres, traduire un texte en temps réel; d'autres encore, créer des adresses électroniques sous la forme d'alias. Par exemple, le widget DNSLytics, de la société du même nom (Dnslytics.com), révèle tous les petits secrets d'un site web (date de création, géolocalisation, etc.). Le widget de SimpleLogin (App.simplelogin.io), de la société suisse Proton, fournit, quant à lui, des e-mails alias, ce qui évite d'avoir à donner sa propre adresse et permet de recevoir les courriels sans afficher sa véritable identité. En cas de fuite, il suffira de détruire l'alias.

4 Privilégier les sites sécurisés

Avant de saisir des informations sensibles sur un site internet, il est bon de vérifier si l'adresse URL comporte bien à côté le dessin d'un cadenas. C'est le signe que cet espace numérique est sécurisé; les informations que l'utilisateur transmettra seront chiffrées, donc non lisibles par un tiers qui se placerait entre lui et le site web. Attention, ce cadenas ne garantit pas l'honnêteté et la sécurité du site lui-même… Rappelons par ailleurs que lorsqu'un internaute surfe via un réseau public offert par un restaurant, un commerce, un hôtel, etc., ces derniers ont le droit, dans le cadre légal du marketing (c'est-à-dire en l'alertant et en respectant le règlement général sur la protection des données personnelles, ou RGPD), de le suivre, d'enregistrer ses habitudes de consommation et de récupérer des données le concernant. C'est pourquoi il est toujours conseillé de recourir à un réseau sécurisé, en passant par exemple par un réseau privé virtuel (VPN) ou par le réseau téléphonique 3G/4G/5G – surtout quand il s'agit d'accéder à son compte bancaire en ligne ! ■

PHOKRATES/ADOBE STOCK

DONNE-MOI TON IP, JE TE DIRAI QUI TU ES

Si l'on souhaite demeurer anonyme sur Internet, la première chose à faire est de protéger son adresse IP, car cette dernière 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 l'adresse IP.

L'IP, qu'est-ce que c'est ?

IP correspond à « Internet Protocol », soit un protocole de transmission des données sur le Web. Une adresse IP *(Internet Protocol Address)* 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 communiquer (recevoir et envoyer des données). Sans trop entrer dans les détails, il en existe deux versions: IPv4 (*Internet Protocol* version 4) et IPv6 (*Internet Protocol* 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'objets connectés grandissant de mois en mois, les adresses IPv6 ont été conçues pour que tous puissent en avoir une. En 2022, selon l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep), la France hébergeait 244 millions d'objets connectés. Et, d'après le cabinet d'études américain IoT Analytics, il y en aurait 14,4 milliards dans le monde, tous disposant d'une adresse IP.

À quoi ça sert ?

Le protocole d'adressage Internet a plusieurs finalités. Outre l'identification des appareils qui se connectent sur la Toile, l'IP sert à diriger (router) les données vers chaque demandeur. Ainsi, les informations arrivent et partent 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,

LEOPATRIZ/ISTOCK

Trouver mon adresse IP

Pour la connaître, rendez-vous sur le site **Adresseip.com.** La page vous l'affichera, ainsi que votre géolocalisation et le serveur utilisé pour router votre IP.

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», en français), qui bloque les connexions provenant d'adresses litigieuses (sites pornos, 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) estime 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).

Sur la Toile, chaque appareil connecté est identifié par une adresse IP unique.

Comment protéger son IP ?

Comme nous venons de le voir, éliminer l'IP de ses connexions sur le Web 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 123.456.7.8. Grâce à cette technique, on peut «faire croire» à un site basé au Canada que l'on est Canadien… Mais rappelons que les éditeurs des VPN savent toujours, eux, qui l'on est vraiment. Et que les versions gratuites ne sont pas recommandées – quand un logiciel ou un service numérique est gratuit, c'est que la société qui le propose se rémunère avec les données de l'internaute qu'elle récolte.

En outre, visiter des sites en HTTPS est indispensable. Le «s» indiquant un chiffrement entre l'utilisateur et le site. Rajouter un VPN permet de cacher son identité au site consulté.

Pour protéger son adresse IP, il est également possible d'exploiter un navigateur dédié. Le plus connu s'appelle TOR (lire p. 84); il peut camoufler une véritable adresse IP par celle d'un ordinateur hébergé dans un autre pays et exploitant le réseau TOR. Des applications pour navigateur, telle qu'uBlock Origin, s'avèrent aussi utiles pour empêcher les sites web visités par l'internaute de le géolocaliser à partir de son adresse IP. Enfin, il est important de rappeler 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 réfléchir à la nécessité de fournir certaines données demandées… ■

SAUVEGARDE EN LIGNE
VOS DONNÉES DANS LE CLOUD

Sauvegarder ses données est aujourd'hui impératif. Et les stocker en ligne demeure la plus pratique des solutions.

Votre smartphone a vu grandir vos enfants, petits-enfants… Il est la mémoire des moments partagés en famille, entre amis. C'est lui aussi le maître de votre vie sociale, puisqu'il renferme vos numéros de téléphone et les adresses de vos proches, de vos médecins, de vos connaissances. Votre ordinateur contient autant de documents aussi précieux, ainsi que des photos, des papiers officiels (factures, avis d'imposition…). Avez-vous déjà imaginé tout perdre ? Panne, vol, virus informatique: vos appareils sont vulnérables ! Mettre vos données à l'abri est impératif; en cas de pépin, vous les retrouverez en deux clics.

Simple et pratique

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. Vous pouvez aussi partager très simplement des documents avec vos proches – des photos de vacances, par exemple. Enfin, et surtout, les outils cloud donnent la possibilité de programmer des sauvegardes automatiques, ce qui assure de toujours disposer d'une copie de ses dossiers, même les plus récents. Certaines vont encore plus loin et proposent des fonctionnalités telles que la gestion des mots de passe, la suppression à distance de fichiers ou la dépose de documents sensibles dans un espace «coffre-fort».

Nous avons testé 12 outils de stockage en ligne plus ou moins célèbres (Dropbox, OneDrive, Google Drive, Apple iCloud… mais aussi pCloud, kDrive, IceDrive, Giga, etc.), en optant chaque fois pour des versions payantes. En effet, celles-ci mettent à disposition 1 ou 2 To d'espace de stockage, quand les offres gratuites n'en proposent que 5 à 20 Go, ce qui ne suffit pas. Vous pourrez toutefois choisir entre une facturation au mois ou à l'année, cette dernière revenant un peu moins cher. Pour pCloud et Internxt, il est même possible de prendre des abonnements «à vie»… tant que vous ne dépassez pas les 99 ans. Et à condition, bien sûr, que l'entreprise ne fasse pas faillite entre-temps ! Ces solutions se déclinent en un logiciel à installer sur ordinateur et une application à télécharger sur son smartphone; on peut ainsi facilement piloter ses fichiers depuis les deux supports. Dropbox s'avère la meilleure de toutes, c'est pourquoi nous l'avons utilisée comme exemple dans notre Pas-à-pas (lire aussi p. 38-39). Elle est cependant talonnée par plusieurs autres, dont OneDrive, Mega Pro ou pCloud.

MARUTSTUDIO/ADOBE STOCK

Test 12 SOLUTIONS PAYANTES

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

		Performances Windows(1)							Performances macOS(2)			Polyvalence	Appréciation globale		Prix
		Configuration	Sauvegarde ponctuelle	Synchronisation de fichiers	Accès aux données à distance	Partage de fichiers	De téléchargement	Vitesse en écriture	Version macOS (2)	Application Android	Application iOS		Note sur 20		€/mois
1	**DROPBOX** PLUS	★★★	★★	★★	★★★	★★★	★★★	★★	★★★	★★★	★★★	★★★	**16,5**	★★★	11,99
2	**ONEDRIVE** MICROSOFT 365 PERSONNEL	★★★	■■	★★★	★★★	★★★	■	★	★★	★★★	★★	★★★	**16,2**	★★★	7
3	**MEGA** PRO I	★★★	■■	★★★	★★★	★★★	★	★★	★★★	★★★	★★	★★★	**16,2**	★★★	9,99
4	**PCLOUD** PREMIUM PLUS	★★★	■■	★★★	★★★	★★	★★	★	★★★	★★★	★	★★★	**15,9**	★★	99,99 (3)
5	**HIDRIVE** PRO	★★★	★★★	★★	★★★	★★★	■	■■	★★	★★★	★★	★★★	**15,6**	★★	24
6	**ICLOUD** +	★★★	■■	★★★	★★	★★★	■	■	★★	n. a.	★★★	★★	**15,4**	★★	9,99
7	**GOOGLE DRIVE** BUSINESS STANDARD	★★★	■■	★★★	★★★	★★★	★★★	★★	★★★	★★	★	★★★	**15**	★★	10,40
8	**KDRIVE** SOLO	★★	■■	★★	★★	★★★	■■	★	★★	★★★	★★	★★★	**14,7**	★★	4,99
9	**ICEDRIVE** PRO	★★	■■	★★★	★★★	★★	★★★	■	★	★	■	★★	**12**	★	4,99
10	**INTERNXT**	★★★	■■	★★★	★	★	■■	■■	★	★★	■	★★	**11,5**	★	9,99
11	**GIGA**	★★★	■	■■	★	★	★★	★★	★	■■	★	★	**9,3**	★	9,99
12	**NORDLOCKER** BUSINESS PLUS	★★	■■	★	★★	n. a.	★	■■	★	■■	n. a.	★	**8,6**	★	14,99

(1) Sur MacOS pour iCloud. (2) Version Windows pour iCloud. (3) Par an.

NOTRE MÉTHODE

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

La meilleure

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

C'est la solution la plus complète et la plus pratique. En plus d'offrir des fonctions de synchronisation, d'accès en ligne et de partage, Dropbox permet de gérer ses mots de passe, d'effacer les données d'un appareil à distance et de signer électroniquement ses documents. Elle est également la seule, avec HiDrive Pro, à autoriser les sauvegardes ponctuelles. Enfin, ses vitesses de transfert de fichiers sont les plus élevées du marché.

L'alternative

kDrive SOLO
4,99 €/mois **14,7/20 | ★★**

Voilà une alternative intéressante aux géantes que sont Dropbox, Google Drive ou OneDrive. Moins connue que ces dernières, kDrive est aussi moins chère. Tout en étant performante sur l'essentiel, que ce soit le stockage, la synchronisation ou le partage de fichiers. Son credo : le respect de la vie privée (les données clients sont stockées en Suisse). Seuls bémols, la sauvegarde manuelle est impossible et les transferts s'avèrent un peu longs.

Pas-à-pas

INSTALLER ET CONFIGURER DROPBOX

● **Objectif :** profiter des fonctions d'un logiciel de sauvegarde sur un ordinateur et un téléphone ● **Niveau de difficulté :** assez facile ● **Temps nécessaire :** 5 à 10 minutes.

La synchronisation, une action à double sens

Avec la synchronisation, un document que vous modifiez sur votre ordinateur sera immédiatement reproduit à l'identique sur votre compte Dropbox, et la version à jour sera accessible depuis tous vos appareils connectés au compte (ordinateur portable ou de bureau, téléphone…). Cette fonctionnalité offre une certaine sécurité: si votre ordinateur tombe en panne, vous disposez de la copie des fichiers, et si vous les effacez par erreur, il reste possible de les récupérer dans la corbeille de Dropbox. En revanche, si vous vous trompez en modifiant un fichier et que vous l'enregistrez ainsi, il n'y aura pas de récupération possible de l'ancien; le nouveau sera immédiatement dupliqué sur le logiciel. La version standard vous permet de synchroniser un seul dossier de votre ordinateur, logiquement nommé «Dropbox». Aucun autre ne peut l'être.

Adaptation : avec ou sans copie sur l'ordinateur ?

Au moment de son installation, Dropbox vous demande comment vous souhaitez synchroniser. «Stocker les fichiers en local» signifie que ces derniers seront conservés deux fois, sur votre ordinateur et en ligne, et mis à jour en permanence; «Stocker les fichiers en ligne», qu'ils ne seront gardés que dans Dropbox (image 1 p. 39). La première manière est généralement la plus pratique, puisqu'elle permet de travailler sur ses documents même sans disposer d'une connexion internet. La seconde façon de procéder n'est intéressante que pour stocker de très grosses quantités de données: si votre ordinateur n'a qu'un petit disque dur, il peut alors exploiter les 2 téraoctets (To) d'espace du compte Dropbox.

La sauvegarde, une reproduction à sens unique

Sauvegarder consiste à conserver une copie de vos dossiers dans le stockage en ligne, afin de les protéger contre une panne ou une erreur de manipulation (image 2). Cela implique de garder aussi ceux supprimés ou modifiés. Par exemple, si vous travaillez sur un fichier Excel et que vous faites 12 versions successives, il y aura 12 fichiers différents dans la sauvegarde, chacun avec leur date d'enregistrement. En cas de pépin, vous pourrez récupérer n'importe quel d'entre eux. Attention, si vos documents sont automatiquement copiés vers le compte Dropbox, l'inverse n'est pas vrai. En cas de perte, vous pourrez toutefois récupérer les différentes sauvegardes via la page internet du logiciel.

Automatique que pour les photos du téléphone

L'appli Dropbox sur smartphone permet également de conserver ses clichés et vidéos (images 5 et 6). À noter: ceci n'est valable que pour les images enregistrées par le téléphone avec l'appli de photographie; celles issues d'applis spécifiques, comme WhatsApp, ne seront pas sauvegardées automatiquement. Il est cependant possible de le faire ponctuellement à la main.

Par **Patrick Gérard** (HC Lab)

Les étapes essentielles

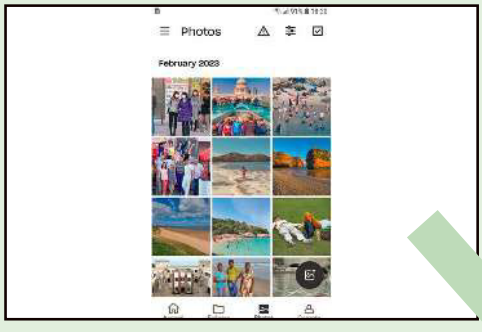
1 Lors de l'installation, il faut sélectionner le mode de fonctionnement de sa Dropbox : les fichiers seront dupliqués sur l'ordinateur et en ligne, ou bien uniquement en ligne.

2 Le choix des documents à sauvegarder est simple : cliquer sur « Modifier la sélection des dossiers » permet d'en ajouter.

3 Dropbox propose tous les dossiers standards de Windows. À ce stade, il n'est pas encore possible d'en sauvegarder un qui soit personnalisé.

4 Sur PC, on peut copier ponctuellement un fichier vers Dropbox. Pour cela, il faut ouvrir la page internet du logiciel et sélectionner « Importer ». On choisit ce que l'on veut copier et puis on clique sur « Importer ».

5 Sur le téléphone, une fois installée, l'appli propose de sauvegarder les photos – toutes, ou seulement les nouvelles. Cette option fonctionne aussi avec les vidéos.



6 S'il y a beaucoup de photos et de vidéos, la première sauvegarde peut être assez longue. Elles apparaîtront ensuite dans la galerie de Dropbox, accessible depuis n'importe quel appareil.

LE MOBILE… DU CRIME

Nos smartphones stockent de plus en plus de ces données personnelles si convoitées par les pirates. Bien protéger son mobile est donc une priorité. On vous dit tout.

Les téléphones de nouvelles générations sont de véritables ordinateurs de poche. Avec toutes les richesses, mais aussi tous les travers que cela implique… En premier lieu, il faut savoir ce qui est stocké dans l'appareil; les données à protéger étant celles relatives à l'identité (nom, adresse, numéro de Sécurité sociale), aux coordonnées (téléphone, adresse électronique), à l'historique de navigation (sites web visités, recherches effectuées), aux photos et vidéos personnelles, à l'historique de messages et d'appels, aux contacts et carnets d'adresses, à la géolocalisation et aux applications (identifiants et mots de passe).

Pour un usage sécurisé

Cela peut paraître anecdotique, mais verrouiller un téléphone portable est indispensable. Si c'est avec un mot de passe, pas question d'en prendre un trop simple à quatre chiffres ! On y ajoute des lettres. Une clé biométrique (empreinte digitale, visage, etc.) constitue une solution intéressante, mais non sans défaut; le mot de passe reste à privilégier. Pour les applications, surtout celles permettant d'accéder aux données sensibles et personnelles, il faut activer la double authentification (2FA). On pensera aussi à utiliser les options de sécurité proposées par le téléphone (dans «réglages»). Selon la marque et la génération de l'appareil, certaines, comme le chiffrement ou la création d'un espace sécurisé et invisible, s'avèrent extrêmement pratiques. Les derniers modèles sous Android, par exemple, proposent des conteneurs chiffrés et illisibles sans un mot de passe, ou encore la reconnaissance faciale du porteur du téléphone.

Verrouiller son smartphone avec un mot de passe fort est une précaution de base.

PEOPLEIMAGES.COM/ADOBE STOCK

Les pratiques à éviter

Mieux vaut ne pas stocker des informations sensibles (numéros de compte bancaire ou de Sécurité sociale) sur un téléphone. Y garder toutes ses photos et vidéos sans les télécharger fréquemment n'est pas non plus recommandé; c'est prendre le risque de ralentir l'appareil et de les perdre en cas de casse ou de vol. Une solution physique pour les ranger, comme un disque dur externe déposé dans un tiroir, chez soi, est préférable à

Connaître l'IMEI de son appareil

Grâce au code IMEI, les opérateurs peuvent bloquer un téléphone signalé comme volé ou perdu, et ainsi l'empêcher d'être utilisé sur leur réseau. Pour le connaître, tapez sur le clavier, en lieu et place d'un numéro, **le code *#06#.**

un service «nuagique» (cloud) proposé par l'opérateur ou le constructeur du téléphone. Enfin, on ne branche jamais son mobile sur une connexion wifi que l'on ne connaît pas.

Bien gérer ses applis

Les applications installées sur nos smartphones sont-elles toutes vraiment utiles et indispensables ? D'abord, avant de les télécharger, lire leur règlement lié à la sécurité des données personnelles est très important. Les boutiques officielles d'applis, comme Google Play ou App Store, présentent ce qu'elles font avec les informations qu'elles récoltent; le premier indique d'ailleurs que *«la sécurité, c'est d'abord comprendre comment les développeurs collectent et partagent (les) données. Les pratiques concernant leur confidentialité et leur protection peuvent varier selon [l']utilisation, [la] région et [l']âge. Le développeur a fourni ces informations et peut les modifier ultérieurement.»* On s'assure également qu'un examen indépendant de la sécurité du logiciel de l'appli a été réalisé – comprenez, par une autre entité que le concepteur.

Ensuite, sur les applications que l'on utilise, on désactive les autorisations d'accès aux données personnelles (géolocalisation, micro, caméra…) quand elles ne sont pas nécessaires. Et on met régulièrement à jour ces applications, en lisant les modifications apportées avant de les valider, car certaines pourraient être plus gourmandes en collecte de données sans vraiment en avertir les utilisateurs réguliers. Bref, on n'installe pas sur son téléphone un jeu vidéo, par exemple, qui aura accès aux SMS, courriers électroniques ou au micro sans une bonne raison, ni une application n'affichant pas que *«les données sont chiffrées lors de leur transfert»* et n'expliquant pas comment demander leur suppression. Enfin, on efface les applis dont on ne se sert plus ! ■

QUE FAIRE EN CAS DE PERTE OU DE VOL

Le plus gros risque, pour un propriétaire de mobile, est de le perdre avec toutes les données qu'il contient. Voici ce qu'il convient de faire en amont ou, sinon, très rapidement au moment de l'incident.

AVANT

- **Téléphone** Attribuez-lui un mot de passe (il doit être suffisamment fort). Faites de même pour la microcarte de stockage si vous en utilisez une.
- **Carte SIM** Modifiez le mot de passe initial en bannissant les « 0000 » et autres dates de naissance.
- **Numéro IMEI** *(International Mobile Equipment Identity)* : notez cet identifiant unique à 15 chiffres attribué à chaque téléphone portable, car il permet de les distinguer. Vous le trouverez sur la batterie et l'emballage de l'appareil, mais aussi en tapant un code directement sur le clavier (lire l'encadré p. 40).
- **Géolocalisation** Activer l'option, elle sera utile en cas de perte ou de vol.
- **Blocage** Activer cette possibilité, voire celle d'effacer le contenu du téléphone.

APRÈS

- **Mots de passe** Changez immédiatement ceux de toutes les applications et services auxquels vous étiez connecté (messagerie, boutiques, appli bancaire…).
- **Signalement de la perte/du vol** Il faut l'effectuer au plus vite auprès de votre opérateur téléphonique.
- **Plainte** En cas de vol, déposez une plainte au commissariat.

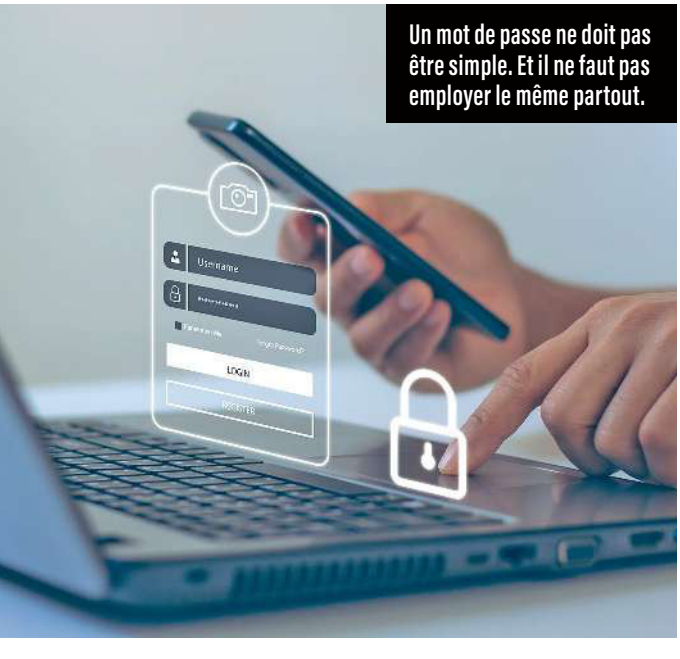
LE MOT DE PASSE, UN SÉSAME ENCOMBRANT

Cette précieuse porte de sécurité protège nos informations des regards non autorisés. Encore faut-il l'avoir « blindée » !

Les mots de passe sont cruciaux. Ils protègent nos informations bancaires, nos e-mails, nos réseaux sociaux… Problème: avec tant de comptes en ligne, difficile de se souvenir de tous. Il est tentant d'utiliser un mot-clé très simple («12345», le nom de son animal, etc.), voire de le réemployer. Ainsi, 65 % des internautes reprendraient le même mot de passe sur plusieurs comptes, selon une étude de Google [1]. Or, cette facilité peut avoir de graves répercussions. C'est comme se promener avec un passe-partout ouvrant sa maison, son journal intime, etc.; si on le perd, gare à la catastrophe.

La phrase, une bonne idée ?

Prendre une phrase comme mot de passe, baptisé aussi «passe-phrase», semble judicieux. Facile à retenir, car tirée de votre livre ou de votre film favori, elle apparaît suffisamment compliquée à trouver par un pirate. Mais il faut savoir que certains sont capables de se renseigner précisément sur un internaute, de lire ses posts et commentaires sur les réseaux, d'en déduire ses passions, ses auteurs fétiches… et de trouver son livre de référence. Cela dit, l'option de la phrase demeure intéressante quand on la modifie quelque peu, en utilisant les initiales des mots, en mettant des chiffres à la place des voyelles, en gardant le signe de ponctuation et la date d'édition, par exemple. La phrase *«Nous plaindre si les Martiens ont mené contre nous une guerre semblable ?»*, tirée de *La guerre des mondes* de Herbert George Wells (1898), pourrait ainsi très bien se transformer en «NpslM4mcn3gs? 1898». Bref, à chacun d'inventer son propre code du moment qu'il se mémorisera bien. Attention, la méthode de substitution, consistant à remplacer voyelles ou consonnes par des chiffres (ici, cela donnerait «N0us pl71ndr3 s1 l3s M4rt13ns 0nt m3n3 c0ntre n0us un3 gu3rr3 s3mbl4bl3 ?»), s'avère bien trop facilement piratable.



Un mot de passe ne doit pas être simple. Et il ne faut pas employer le même partout.

Chiffres et caractères spéciaux à combiner

Comme nous venons de le voir, mixer lettres, chiffres et caractères spéciaux est incontournable, car cela complique beaucoup la tâche du pirate. Les personnes malveillantes utilisent en effet, dans la grande majorité des cas, des logiciels dédiés à «cracker» (pirater) un mot de passe. Ces outils fonctionnement notamment par incrémentation – c'est-à-dire en testant, lettre par lettre, chiffre par chiffre et signe par signe, toutes les solutions possibles jusqu'à trouver le bon sésame. Dès lors, autant dire que plus le mot de passe choisi est biscornu, plus il comprend de caractères spéciaux (signes de ponctuation, etc.), de chiffres et de mix

THAWEERAT/ADOBE STOCK

entre lettres majuscules et minuscules, plus il devient compliqué de le trouver via cette méthode automatisée. De fait, selon le site luxembourgeois Bee Secure [2], le mot de passe «NpslM4mcn3gs?1898» ne serait piraté que dans 108 000 ans !

Mots courants et données personnelles : à éviter

Comme pour certaines phrases trop aisées à deviner, les mots de passe tels qu'«azerty» ou «123456», trop courants, ne sont pas recommandés. De fait, selon un rapport du Département de la sécurité intérieure américain, la moitié des 10 mots de passe les plus utilisés au monde contiennent le mot «password» et la séquence «1234»… Malvenues également: des informations personnelles comme le nom, l'adresse ou la date de naissance, car elles sont bien trop faciles à retrouver (sur les réseaux sociaux en particulier). Enfin, en cas de doute sur la solidité de son mot de passe, il est possible de le tester sur le site du ministère de l'Économie [3], et de découvrir s'il est déjà dans les mains de pirates informatiques, car volés à d'autres personnes.

Le coffre-fort, un bon plan

Un gestionnaire de mots de passe, également appelé coffre-fort, permet de stocker en toute sécurité les clés de ses comptes en ligne, directement sur sa machine (le mieux) ou sur le web (déconseillé). Cet outil est aussi capable de fournir les bons identifiants de connexion au bon site, sans que l'on soit obligé de les retenir par cœur ni de les taper. Attention, un mot de passe «maître» reste obligatoire pour valider le fait que l'on est bien propriétaire du coffre-fort et de son contenu. Il existe plus d'une vingtaine de ces solutions, gratuites et payantes, sur le marché [4], dont KeePass, LastPass, Dashlane ou 1Password, qui proposent également de générer des mots de passe complexes aléatoires. À noter que KeePass (gratuit) est certifié par l'Agence nationale de sécurité des systèmes d'information (Anssi) depuis 2011.

La diversification, le geste malin

Les mots de passe employés dans un cadre privé doivent absolument être différents de ceux exploités dans un contexte professionnel. Au sein d'une entreprise, le service informatique a intérêt à former les salariés à la question (choix du mot de passe, durée de vie, etc.). Dans tous les cas, à la maison comme au travail, il est fortement conseillé d'en changer régulièrement – tous les 45 jours selon les plus prudents ! L'Anssi, de son côté, recommande de procéder à un renouvellement tous les trois à six mois, afin d'empêcher des pirates ayant éventuellement mis la main sur vos informations de conserver un accès non autorisé à vos comptes.

Deux impératifs, pour finir: 1. Il faut sensibiliser ses proches, amis et famille, à la bonne gestion des mots de passe; 2. Il est crucial de ne jamais les partager avec qui que ce soit, même si l'on fait confiance à une personne. Une divulgation accidentelle est en effet toujours possible… Par exemple, sachant que le mot de passe d'une box internet est écrit sur l'étiquette collée à l'arrière du boîtier, comment être certain d'en avoir gardé la maîtrise si on ne le change pas ? ■

PIRATAGE QUANTIQUE

La puissance des ordinateurs évolue vers le quantique, un mode de calcul ultrarapide. Cette vitesse fait peur, au point que le gouvernement américain a voté une loi, la Quantum Computing Cybersecurity Preparedness Act, en janvier 2023, pour protéger les systèmes et les données du gouvernement fédéral contre des menaces de violation utilisant la technologie quantique. Il faut dire que quelques jours auparavant, des experts chinois annonçaient avoir réussi le piratage d'un algorithme considéré comme ultra-sécurisé, le RSA (cette protection apparaît dans votre navigateur sous la forme du petit cadenas et du «s» dans l'adresse «https»). Votre banque, par exemple, utilise cet algorithme et son protocole, baptisé SSL.

(1) Services.google.com/fh/files/blogs/google_security_infographic.pdf.
(2) Pwdtest.bee-secure.lu.
(3) Ssi.economie.gouv.fr/motdepasse.
(4) Wikipedia.org/wiki/Liste_des_gestionnaires_de_mots_de_passe.

LE CAS SNAPCHAT

Saviez-vous qu'il était possible de retrouver vos anciens avatars sur ce réseau ? Nos conseils pour y naviguer en toute tranquillité.

Snapchat, le réseau social préféré des adolescents, permet le partage éphémère de photos et de vidéos. Il a été créé en 2011 par trois étudiants américains, Evan Spiegel, Bobby Murphy et Reggie Brown. Ayant constaté que les clichés envoyés via les réseaux sociaux étaient rarement flatteurs, ils ont eu l'idée d'une application où ces contenus disparaîtraient définitivement après quelques secondes de visionnage. Snapchat était né. Utilisée surtout par les jeunes, cette application de messagerie et de partage est rapidement devenue très populaire dans le monde. Au point qu'en 2013, Facebook a proposé de la racheter pour 2,8 milliards d'euros ! Une offre refusée par Evan Spiegel.

Des contenus réellement éphémères ?

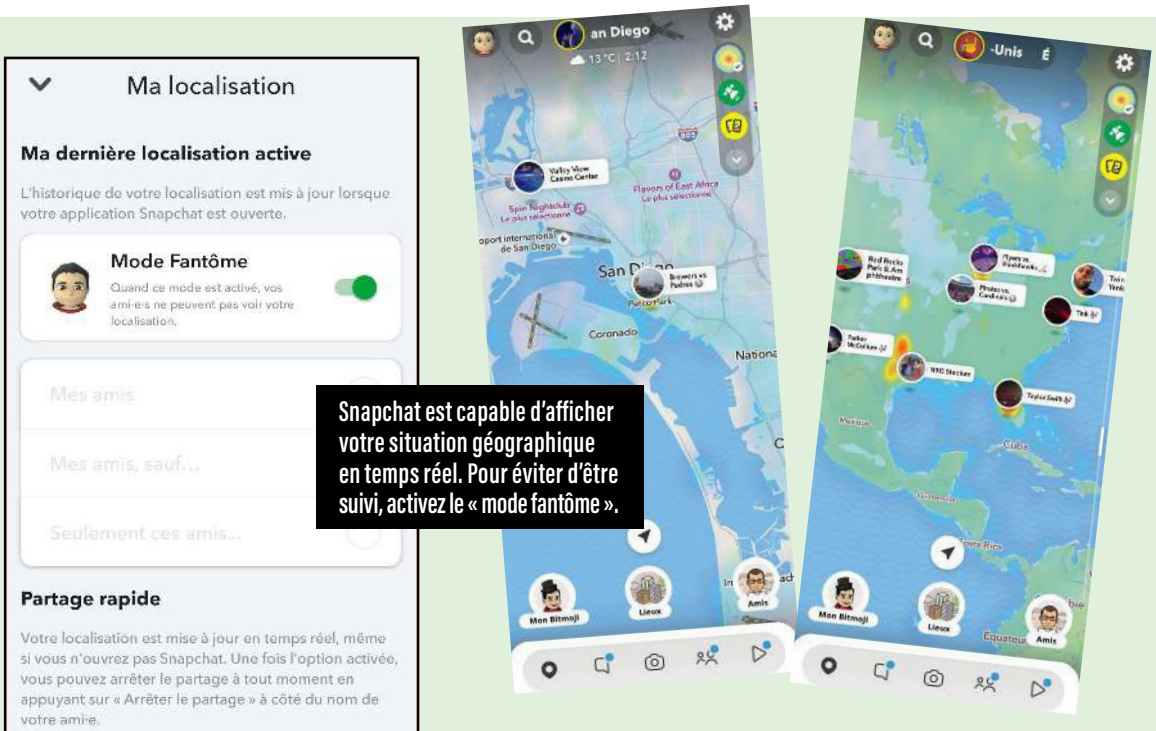
Principal intérêt de Snapchat, photos et vidéos partagées disparaissent après avoir été regardées, et leur diffuseur (propriétaire) peut configurer son application pour être alerté si une sauvegarde ou une copie d'écran est réalisée. Cet outil ludique est également connu pour ses filtres (masques amusants, réalité augmentée, etc.), qui donnent la possibilité d'ajouter, gratuitement ou en payant, des éléments virtuels aux clichés. Snapchat présente toutefois des risques. D'abord, les utilisateurs peuvent être tentés de partager des contenus inappropriés ou illégaux, pensant qu'ils ne seront plus visibles après visionnage… Or, les destinataires ont toujours la possibilité de prendre des captures d'écran ou d'enregistrer des vidéos, ce qui rend les informations permanentes. De plus, dans certains pays, les données issues des réseaux sociaux demeurent stockées sur les serveurs de l'éditeur de l'appli, la loi l'imposant, et ce pour une durée indéterminée. «*Les Snaps et les Chats*

MCLITTLE STOCK/ADOBE STOCK ; KOVOP58/ADOBE STOCK

envoyés dans le Snapchat seront automatiquement supprimés par défaut de nos serveurs après qu'il est établi qu'ils ont été ouverts par tous les destinataires ou qu'ils ont expiré, explique l'entreprise. *D'autres contenus, comme les messages Story, sont stockés plus longtemps.»* C'est notamment le cas des anciens avatars… Explication: quand on ouvre un compte, on se crée un personnage numérique (avatar) pour l'illustrer. On peut ensuite l'habiller, l'installer devant tel ou tel fond d'écran, le faire évoluer selon son humeur, sa zone géographique, etc. Mais les précédentes images ne disparaissent pas! Pour les récupérer, il faut sélectionner l'adresse web de son avatar (qui ressemble à ceci: Images.bitmoji.com/3d/avatar/201714142-162274544_7-s4-v1.webp), puis modifier le chiffre après le tiret bas (le trait sous le chiffre 8 de votre clavier PC).

Conservation des données réglementée

Même les applis promettant la sécurisation de ce qui est diffusé sont tenues de respecter le Règlement général sur la protection des données (RGPD) en matière de conservation des informations. Il en va de même pour Snapchat. Le petit fantôme jaune garde donc les informations d'un compte – nom, numéro de téléphone, e-mail – et la liste des amis jusqu'à ce que leur propriétaire demande leur suppression. Également stockées: les données de localisation, pour des durées différentes selon leur précision et les services utilisés. Celles associées à un Snap (enregistrées dans Memories ou publiées sur Spotlight) seront conservées aussi longtemps que celui-ci. Il est possible de voir ces données en les téléchargeant dans son administration, via Accounts.snapchat.com. Dernier point important: on active le «mode fantôme» quand on ne veut pas qu'il soit possible de géolocaliser l'emplacement et les lieux d'où l'on diffuse photos et vidéos (on peut aussi programmer ce mode pour une durée déterminée). Attention: les Snaps envoyés dans la carte Snap y apparaissent toujours, quels que soient les paramètres de localisation choisis… ■



Snapchat est capable d'afficher votre situation géographique en temps réel. Pour éviter d'être suivi, activez le « mode fantôme ».

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.

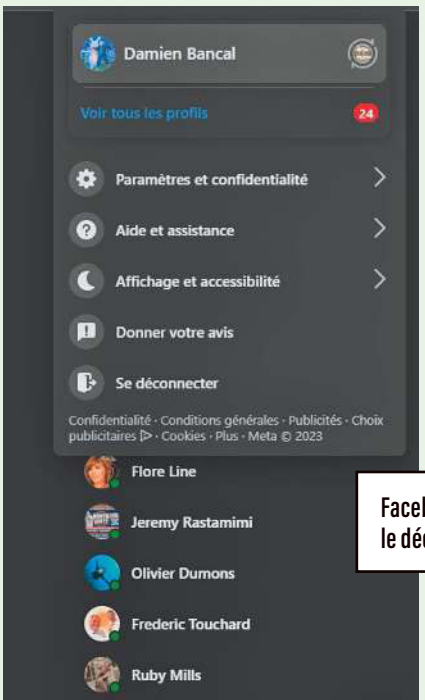
Université de Harvard, États-Unis, 2004. Plusieurs étudiants en informatique, dont Mark Zuckerberg, veulent lancer un réseau social pour communiquer et rester en contact avec leurs camarades. Ils inventent The Facebook, dont le succès dépasse rapidement leur campus pour s'inviter dans des dizaines d'universités américaines, puis bien au-delà… Aujourd'hui, avec 40 millions d'utilisateurs en France, 420 millions en Europe et 2,958 milliards dans le monde (chiffres de janvier 2023), ce réseau social du groupe Meta (lire l'encadré p. 48) est un géant du stockage de données personnelles. Mais tous en sont-ils bien informés ?

Avoir la confidentialité à l'œil

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 comme votre date de naissance, votre adresse mail ou votre numéro de téléphone. Jetez régulièrement un œil sur les règles, car Facebook, lors de ses mises à jour, peut décider du jour au lendemain 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 pas ! Comme vous avez déjà pu le lire p. 42-43, pour qu'il soit



Facebook connaît votre vie par cœur. Vous pouvez le découvrir dans les options « Votre historique ».

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 devient payante, il demeure possible de recevoir son code 2FA via son application téléphonique ou des outils dédiés (comme ceux présentés p. 22). Vous pouvez la configurer en cliquant sur « Paramètres et confidentialité > Sécurité et connexion > Utiliser l'authentification à deux facteurs ».

Gare aux faux amis

Le côté positif du réseautage, c'est qu'il permet de retrouver des proches et des amis perdus de vue, mais aussi de faire connaissance avec des inconnus ayant la même passion, les mêmes centres d'intérêt, etc. Cependant, et d'autant plus sur Facebook, gardez votre bon sens en alerte et fuyez les demandes de personnes que vous ne connaissez pas. Les escrocs pullulent et peuvent recourir à de faux comptes pour accéder à vos informations personnelles. Il est également important de signaler ceux qui vous paraissent suspects à Facebook. Pour avoir une idée de la menace, sachez que Meta a détruit 1,3 milliard de faux profils sur sa plateforme Facebook entre les mois d'octobre et de décembre 2020. Et il y en a encore beaucoup, malgré les 20 000 critères d'analyses du réseau social et les 35 000 modérateurs qui ont pour mission de lutter contre les faux comptes. Il en va de même pour les applications que vous autorisez sur votre compte Facebook. Évitez ces jeux ou ces questionnaires, qui peuvent paraître amusants au premier abord mais 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 ! >>

RETROUVEZ VOTRE « HISTOIRE » FACEBOOK

Vous souhaitez connaître ce que Meta sait de vous ? Retrouver tout ce qui a été diffusé sur le réseau social Facebook concernant votre vie ? 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 »**. Vous avez alors sous les yeux la liste de toutes les recherches que vous avez effectuées sur Facebook depuis la création de votre compte, triées par ordre chronologique. Pour supprimer une recherche spécifique, survolez-la avec votre curseur et cliquez sur « Supprimer », à droite. Concernant l'historique de votre parcours sur Facebook, une fois connecté à votre compte, sélectionnez **« Paramètres et confidentialité > Paramètres »**. Dans le menu de gauche, sélectionnez **« Vos informations Facebook »** puis cliquez sur **« Télécharger vos informations »** : une liste de catégories d'informations que vous pouvez télécharger apparaît. Cochez celles que vous souhaitez recevoir. Il est également possible de sélectionner une plage de dates pour celles que vous voulez inclure. Il faut ensuite un certain temps pour que les fichiers soient générés – selon la quantité de données demandée. Lorsque cette archive est prête (il arrive qu'elle soit très lourde), une notification vous invite à la télécharger. Pour en savoir plus : **Facebook.com/help**.

>> Faire attention 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 les paramètres de confidentialité de vos publications et 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 pour les « J'aime » (« Like ») et les autres commentaires que vous laissez. Attention, d'aucuns peuvent les utiliser pour vous retrouver, et 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 (toujours dans l'espace d'administration de votre compte) qui peut vous voir en utilisant les paramètres de confidentialité de la recherche, mais également qui est en mesure de vous envoyer des demandes d'amis ou des messages. Il en va de même pour les liens reçus sur Facebook et Messenger (le système de messagerie instantanée du réseau social) : il vous faut les paramétrer.

Vérifier les autorisations d'accès

Lorsque vous vous servez d'une application tierce sur Facebook, il est important de jeter un œil sur ses accès à vos informations personnelles – vous le ferez en cliquant sur « Paramètres et confidentialité > Applications et sites web > Autorisations d'application ». C'est d'ailleurs ici que vous trouverez la liste des applis ayant accès à votre compte Facebook et découvrirez les informations dont elles ont connaissance. Supprimez-leur ces accès si vous ne les utilisez plus. Bref, vous l'aurez compris, ce réseau social que l'on aime tant détester continue d'être très présent dans nos vies, que nous le voulions ou non. Il faut donc le gérer avec le plus grand sérieux… ■

*« Facebook vous regarde ! » *(référence au personnage de Big Brother dans le roman* 1984 *de George Orwell, aujourd'hui symbole de ce qui porte atteinte à la vie privée des individus.)*

META, PIEUVRE AVIDE DE DONNÉES PERSONNELLES

La maison mère de Facebook regroupe d'autres outils de réseautage qui réclament toute votre attention. En 2012, Facebook rachète Instagram, une application de partage de photos populaire. En 2014, c'est au tour de l'application de messagerie instantanée WhatsApp. Puis d'Oculus VR, une entreprise de technologie dédiée à la réalité virtuelle. Par ce biais, ce qui est devenu le groupe Meta tente de faire basculer le monde dans le « Metaverse », mais sans grand succès pour le moment.

SUPPRIMER DÉFINITIVEMENT SON COMPTE FACEBOOK

Dorénavant, il est possible de supprimer son compte quand on veut quitter le réseau social de Meta. Pour cela, il faut cliquer sur sa photo de profil, sélectionner **« Paramètres et vie privée »** dans le menu, puis cliquer sur **« Paramètres > Espace Comptes > Informations personnelles > Propriété et contrôle du compte > Désactivation ou suppression ».** Cette opération peut être annulée pendant 30 jours ; après, il est trop tard. Votre profil, vos photos, vos publications, vos vidéos, ainsi que tous les éléments que vous avez ajoutés seront définitivement effacés. Attention, si vous avez utilisé Facebook pour vous connecter à d'autres applications (mobile ou via votre ordinateur), vous ne pourrez plus accéder à ces dernières (jeux, etc.). Et les messages que vous avez envoyés à vos amis demeurent visibles pour ces derniers une fois votre compte supprimé.

SOYEZ CYBER-PROTECTEUR

Vous devez collecter les données personnelles d'autrui ? Voici quatre conseils pour le faire correctement.

1 BIEN COLLECTER, C'EST UN DEVOIR

Les entreprises sont tenues de respecter de nombreuses règles, formalisées dans le RGPD, quand elles collectent des données personnelles. De leur côté, les particuliers doivent se plier à une certaine hygiène numérique pour ne pas collecter ce qui n'a pas à l'être. Par exemple, s'ils fondent une association et demandent à leurs adhérents des informations (leur emploi, leur médecin…), il faut qu'ils s'assurent, comme le rappel la Cnil, 1. que ce soit nécessaire pour atteindre leur objectif; 2. que ce dernier soit légitime, bien défini et explicable aux personnes concernées; 3. que les données récoltées ne puissent pas être employées ultérieurement de façon incompatible avec ce but initial.

2 MAÎTRISER L'APRÈS-COLLECTE

Collecter noms, prénoms, adresses et téléphones peut paraître anodin. Mais cela implique de maîtriser ensuite le stockage, l'usage, la modification, la destruction et la restitution de ces informations; bref, d'en conserver le contrôle. Ceux dont on récupère les données doivent donc être prévenus (il est interdit de le faire à leur insu) et informés de leur utilisation, mais aussi de leurs droits et des moyens de les exercer. S'il s'agit de mineurs, l'accord d'un représentant légal est requis.

3 DÉFINIR UNE DURÉE DE DÉTENTION

Pour une collecte éthique et respectueuse du droit, il faut définir une durée de conservation des informations, car elles ne peuvent être gardées indéfiniment. Par exemple, dans le cas d'une association, les fiches d'inscription ne seront maintenues en gestion courante que pour une période prédéfinie – en général, une année. À l'issue de celle-ci, elles seront détruites, anonymisées ou bien archivées, en accord avec les obligations légales en matière de conservation des archives publiques.

Pour collecter des données, certaines règles sont à respecter.

SEVENTYFOUR/ISTOCK

4 SÉCURISER LE STOCKAGE

La sécurité «physique» et informatique des éléments de stockage (cloud, serveur NAS, disque dur, etc.) doit être assurée pour éviter vols et intrusions. Ainsi, locaux, armoires et postes de travail seront verrouillés pour empêcher tout accès non autorisé. Il est également essentiel d'encadrer la consultation des données (qui peut ou ne peut pas le faire) et de les catégoriser, car toutes ne sont pas aussi sensibles (par exemple, l'âge l'est moins que l'adresse postale). Ce qui induit d'adapter les protections à la nature des informations conservées (utilisation du chiffrement, d'un coffre-fort pour le disque dur, etc.). Enfin, on n'oublie pas de réaliser une sauvegarde afin de pouvoir récupérer les fichiers en cas de sinistre (dégâts des eaux, incendie, piratage, etc.). ■

SOMMAIRE

Éviter les arnaques

Faux courriels de votre banque, sites cherchant à vous piéger, interception des données de votre téléphone, infiltration de l'ordinateur familial, liaisons amoureuses bidon, virements frauduleux… voilà quelques exemples de menaces en ligne que nous allons décortiquer dans ce chapitre. Ils démontrent l'imagination débordante des pirates du Web, le caractère protéiforme de leur malveillance, mais aussi l'intensité de leurs attaques. De fait, selon une étude de l'Insee de 2020, la moitié des habitants de l'Union européenne déclarent qu'un ou plusieurs membres de leur famille ont déjà vécu une arnaque ou été victimes d'un piratage. Ainsi, 35 % des personnes interrogées auraient été ciblées par d'une tentative d'hameçonnage et 30 % auraient découvert un logiciel espion dans leur PC. En outre, d'après le site Cybermalveillance.gouv.fr, en France une fraude bancaire touche un particulier toutes les quatre secondes, et le piratage de comptes en ligne a fait un bond de 139 % en 2021…

GRAPHICROYALTY/ADOBESTOCK

LES PIÈGES LES PLUS FRÉQUENTS

Il existe de nombreux types de cyberattaques, mais certaines sont plus courantes que d'autres. En voici quelques-unes que vous trouverez un jour ou l'autre sur votre chemin numérique.

L'HAMEÇONNAGE (PHISHING)

Cette tentative 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.

Gare aux 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 malveillants, 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 2022, celui concernant l'adresse de l'assurance maladie (Ameli.fr). Les fraudeurs avaient découvert que dans un SMS, le «I» majuscule ressemblait beaucoup au «l» minuscule. Bilan, le site Ameli.fr était écrit AMEIi.fr (Ameii.fr)…

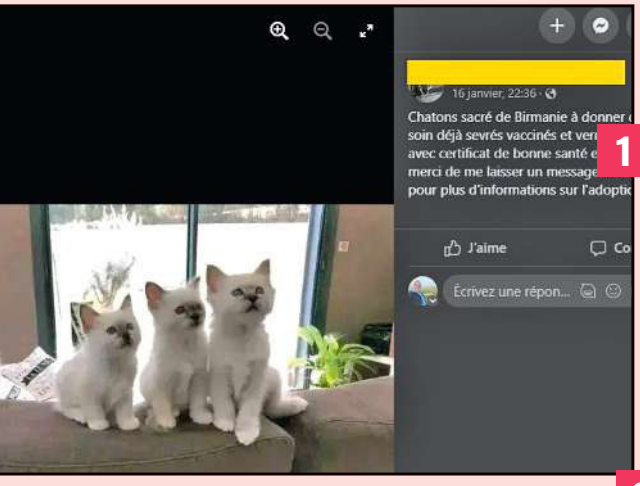
L'enregistrement d'un nom de domaine proche de celui d'un site connu mais avec quelques lettres modifiées est également fréquent. Citons Chrronopost.fr, Netfliix.fr, Vignettesair-gouv.fr. Autre cas possible (mais il en existe encore beaucoup): la création d'un nom de domaine qui n'appartient pas à l'entreprise, 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».

Fausses URL référencées

Red.flag.domains répertorie les adresses de sites malveillants acquises par des pirates, soit plusieurs centaines de .fr par mois !

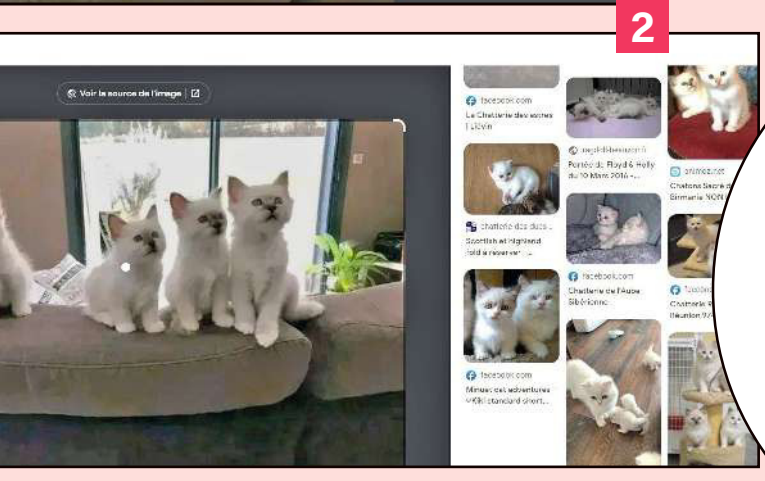
LES FAUSSES PETITES ANNONCES

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 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.



1

Une petite annonce propose d'adopter des chatons Si l'on enregistre la photo qui l'illustre puis qu'on la glisse dans la fenêtre de Google Images pour analyse **(1)**, on découvre qu'elle apparaît sur d'autres plateformes et d'autres annonces **(2)**. Ici, le cliché des chats, soi-disant nés en juillet 2022, provient en réalité du site d'un éleveur **(3)** dont les chatons ont vu le jour en… 2019.



2

3

> **L'arnaque au chaton** Un particulier publie sur Facebook la photographie d'adorables 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 et d'un vaccin. Le coût ? Entre 80 et 250 €. Une page de transaction est envoyée pour le paiement. Mais le chat, lui, n'arrivera jamais, car il n'existe pas ! En plus de l'argent de ses victimes, l'escroc aura collecté leurs données personnelles et celles de carte bancaire.

> **Le placement miraculeux** Ces arnaques consistent à inciter les gens à investir 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, les rendements de 25, 50, voire 100 % n'existent pas.

> **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 encore « *J'ai piraté ton PC* » ? Depuis quatre ans, ces tentatives d'extorsions explosent. Les escrocs 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 leur silence, le criminel réclame quelques centaines d'euros. C'est du bluff, il n'a rien infiltré. Mais l'affolement pousse certains particuliers à payer. >>

LE LIEN MALVEILLANT

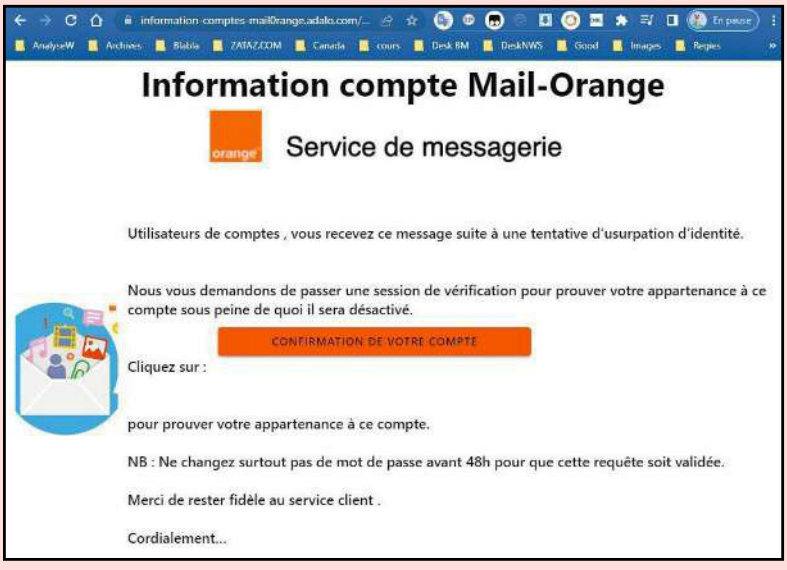
Vous avez un blog sur lequel vous partagez vos passions et centres d'intérêt. Il vous arrive d'y diffuser des liens vers d'autres espaces numériques. Un jour, vous recevez un courriel d'un inconnu, qui vous explique que votre dernier post est génial mais que l'adresse web indiquée n'est plus valide, 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.

L'INFILTRATION DES ESPACES PRIVÉS

En infiltrant 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 l'administration fiscale. Ainsi, par le biais d'un phishing, entre autres, le malfaiteur réussit à prendre la main sur votre compte créé sur le site du Trésor. Il modifie le montant, en y ajoutant, par exemple, des dons à des associations, l'emploi d'une nounou, d'un jardinier… Son idée ? Profiter du dégrèvement fiscal et récupérer le remboursement des impôts. L'argent lui sera alors envoyé par lettre chèque à l'adresse modifiée à cet effet, ou versé sur un compte bancaire ouvert pour l'occasion.

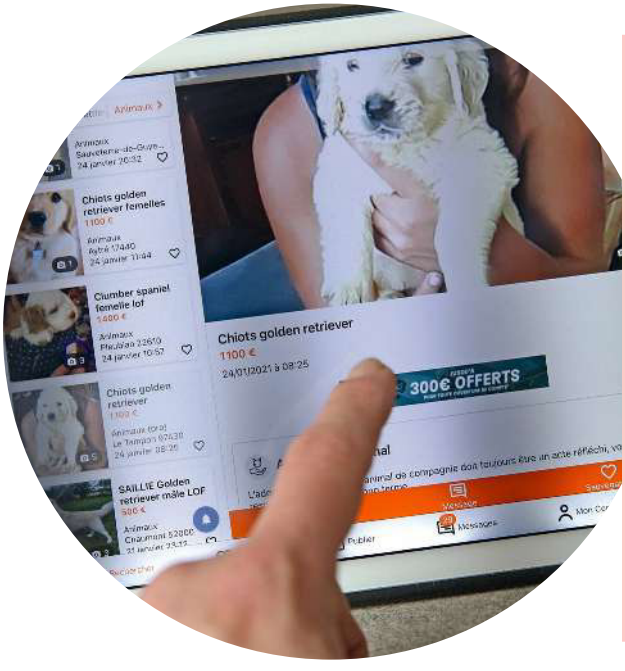
BAILLEUR QUELS DOCUMENTS PEUT-IL EXIGER ?

Le législateur a établi la liste des documents qu'un propriétaire est autorisé à réclamer à un candidat à la location : une seule pièce d'identité en cours de validité, un seul justificatif de domicile, une ou plusieurs attestations de situation professionnelle, un ou plusieurs justificatifs de ressources. Vous trouverez, sur **Service-public.fr/particuliers/vosdroits/F1169,** la liste complète des pièces exigibles. Consultez-la avant de répondre à n'importe quelle demande.



Vous recevez un courriel aux couleurs de votre opérateur

Inquiétant, il évoque une tentative d'usurpation d'identité et vous incite à révéler vos identifiants sous prétexte d'une vérification… Mais tout est bidon, comme le prouve l'URL dans la barre d'adresse, qui n'est pas la bonne.



LES RÈGLES D'OR

- **Ne croyez pas à une offre qui semble trop belle** pour être vraie, il s'agit probablement d'un piège.
- **Ne fournissez jamais d'informations personnelles** sensibles et ne faites aucun paiement à des personnes ou à des entreprises que vous ne connaissez pas.
- **Effectuez des recherches et vérifiez** à qui vous avez affaire avant de donner suite à une proposition.
- **Maintenez vos logiciels de sécurité à jour** sur votre ordinateur.
- **Abstenez-vous toujours de cliquer** sur des liens douteux.

LES JUSTIFICATIFS DE RECHERCHE DE LOGEMENT

Vous êtes en quête d'un logement à louer et une petite annonce attire votre attention. Votre interlocuteur, que vous avez contacté par téléphone et par courriel, semble fiable et sérieux. Une fois la confiance installée, il vous réclame un certain nombre de pièces pour cet appartement que vous convoitez. N'envoyez rien par courriel ! Cet aimable propriétaire pourrait bien être un escroc dont l'unique objectif est de vous soutirer un maximum d'informations personnelles afin de s'en servir ensuite (pour 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, baptisé Dossierfacile.fr, 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 ! Le propriétaire ne peut réclamer que les pièces dûment autorisées (lire l'encadré ci-dessus), sans quoi il encourt 3 000 € d'amende (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 d'exiger la présentation de l'originale.

LES FAUX COURS PARTICULIERS

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 d'économie, de mathématique, etc., contre paiement. Les cours ont bien lieu, la confiance s'installe mais, petit à petit, l'élève va poser à son professeur des questions sur son emploi, ses activités, etc. En réalité, il s'agit d'infiltrations menées par des agents des services secrets russes ! *« 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 les services de contre-espionnage. *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 également été employée avec des étudiants à la recherche d'un stage. Les futurs responsables réclament, par exemple, que les candidats leur fournissent lors d'une rencontre des rapports de stages effectués dans d'autres entreprises… ■

F. FREY/I'ALSACE-MAXPPP

CRIT'AIR SÉDUIT LES ESCROCS

L'arnaque à la vignette automobile Crit'Air est omniprésente sur Internet. Explication.

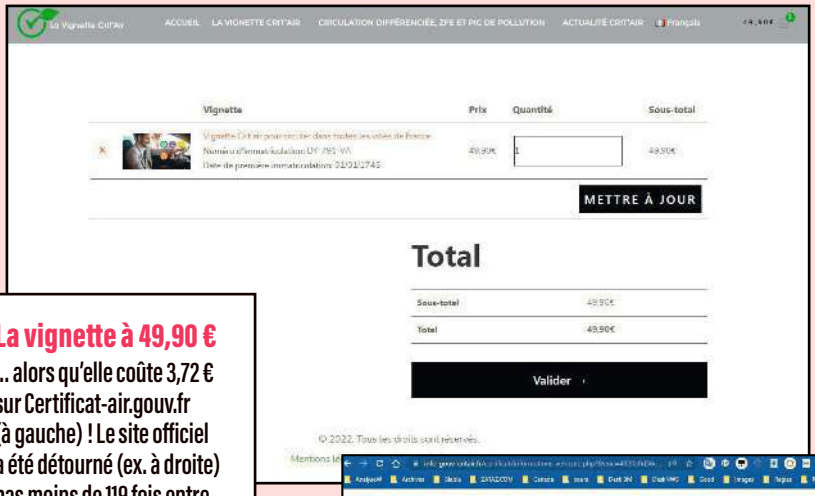
La vignette Crit'Air a été instaurée dans de nombreux pays européens afin de réguler le flux des voitures dans les grandes villes et d'y combattre ainsi la pollution. En France, elle est apparue en 2016. Obligatoire pour circuler dans les zones à faibles émissions mobilité (ZFE-m), progressivement instaurées dans les agglomérations, elle sert à classer les véhicules en fonction de leurs rejets polluants. Pour l'acquérir, il faut se connecter au site officiel créé par le gouvernement. Son adresse: Certificat-air.gouv.fr. C'est la seule plateforme habilitée à délivrer la précieuse pastille, mais les pirates et autres profiteurs du Web ont compris qu'il y avait là aussi de l'argent à se faire.

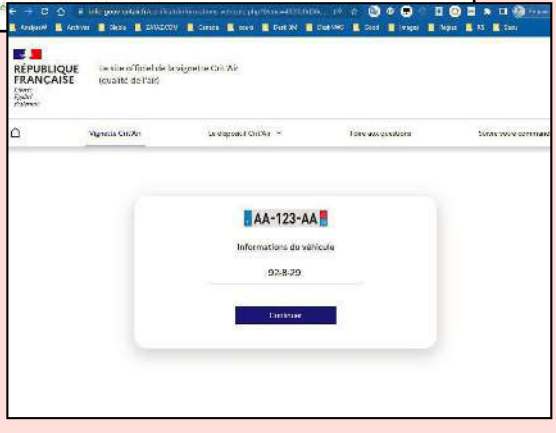
De faux sites par centaines

Entre le 1er et le 22 janvier 2023, pas moins de 119 faux sites Crit'Air ont été découverts, à visée commerciale ou de phishing. Dans le premier cas, des professionnels malhonnêtes jouent sur l'ignorance des internautes et sur le référencement payant des moteurs de recherche pour faire apparaître, en tête des requêtes, leur site (qui met bien en avant la vente de Crit'Air dans sa dénomination). Leurs boutiques permettent effectivement d'acheter la vignette, mais à un prix nettement plus élevé que le tarif officiel. Certains facturent ainsi 49 € le document à coller sur votre parebrise, alors qu'il ne coûte que 3,72 € (3,11 € + 0,61 € d'affranchissement) sur Certificat-air.gouv.fr ! Ils expliquent ce surcoût par le travail administratif qu'ils ont fourni pour acheter la vignette…

COMMENT ÉVITER LES SITES FRAUDULEUX

Les produits et services d'un site vous tentent ? Restez vigilant. Avant de lui fournir vos données personnelles et votre numéro de carte bancaire, vérifiez certains éléments. D'abord, l'URL. L'adresse est-elle correcte ? Connue des moteurs de recherche (Bing, Google, Qwant, etc.) ? Cohérente avec le contenu du site ? Le https et son petit cadenas ne garantissent pas que la plateforme est honnête, ils indiquent juste une connexion sécurisée entre elle et vous. Ensuite, la présentation. Design impeccable, navigation facile et absence de fautes de français sont des signes positifs. À l'inverse, des pages à l'orthographe douteuse, entre autres, doivent alerter. Enfin, les informations sur l'entreprise ou le gestionnaire du site sont essentielles : adresses électronique et physique, numéros de téléphone et d'identification fiscale (Siren/Siret) et formulaire de contact doivent être présents et faciles à trouver et à vérifier. Si ce n'est pas le cas, cela ne sent pas bon ! Dernier point : cherchez et lisez les avis des usagers (sur Google, par exemple), en gardant à l'esprit que certains messages peuvent être faux ou manipulés. Il convient donc de s'assurer que les commentaires sont réalistes.





La vignette à 49,90 €
... alors qu'elle coûte 3,72 € sur Certificat-air.gouv.fr (à gauche) ! Le site officiel a été détourné (ex. à droite) pas moins de 119 fois entre le 1er et le 22 janvier 2023.

Dans le cas du site de phishing, aucun service ne sera rendu. L'objectif des escrocs est de collecter vos données personnelles (plaque d'immatriculation, adresse électronique, informations bancaires…) afin de vous voler ou de se faire passer pour vous. Certains n'hésitent pas à exiger des pièces justificatives officielles. Or, sachez-le, jamais le véritable site Crit'Air ne vous réclamera un permis de conduire ou une carte nationale d'identité (CNI) pour vous vendre une vignette.

Méthodes bien rodées

Pour leurs faux sites, les pirates exploitent la plupart du temps les mots suivants: authentification, certificat, .gouv, etc. Ils mettent en place des variantes, rajoutant ou retirant des lettres, inversant des phrases, etc. On trouve ainsi des Service-critair.fr; Info-gouv-critair.fr; Critairs-authentification.fr; Regulation-critair.fr; Critair-paiement-gouv-fr.com… Ces adresses frauduleuses ont une durée de vie très limitée car les autorités les font fermer rapidement. Afin de contourner cette difficulté, les malfaiteurs agissent sur une période courte – en général, dès qu'une grande ville annonce la mise en place d'une ZFE. En effet, à peine l'information a-t-elle été diffusée par les médias que des milliers d'automobilistes se ruent sur Internet pour commander leur vignette Crit'Air. C'est donc le moment qu'attendent les escrocs pour piéger les internautes ignorants ou peu vigilants. Ils utilisent pour cela plusieurs méthodes, la plus rapide étant celle des publicités en ligne. Ces spots vont apparaître avant le site officiel gouvernemental, à une date et une heure précise, par exemple celle du journal télévisé où le sujet des zones à faibles émissions sera traité, car il fait partie de l'actualité. Il suffit aux pirates d'une phrase d'accroche pour que les internautes n'aillent pas plus loin dans les propositions des moteurs de recherche. Quelques exemples: «*Attention, dans plusieurs villes de France la vignette est obligatoire pour circuler*»; «*Prudence: Bordeaux, Lille, Lyon et d'autres communes imposent la vignette*»; etc.

Il en va de même avec les messages frauduleux concernant Crit'Air envoyés par courriel ou SMS: ils sont expédiés pour inciter des particuliers sans méfiance à se rendre sur les sites de phishing. La loi Climat et Résilience de 2021 prévoit que, d'ici à 2025, 43 villes de plus de 150000 habitants seront dotées d'une ZFE. Les attaques des cyberpirates risquent donc fort de continuer ! ■

VOS DONNÉES SE REVENDENT AU MARCHÉ NOIR

Trouver des données piratées sur le web et le darknet n'est plus très compliqué. Les boutiques qui vendent des informations volées n'ont jamais été aussi nombreuses. Découverte d'une activité florissante.

Prénommé Karys (un pseudonyme), il est 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 très bien être Belge, Français, Canadien ou Chilien. Depuis cinq ans, il vit 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. *«J'ai commencé car j'avais 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.

Il y aura toujours des acheteurs

Aujourd'hui, Karys dispose de plusieurs boutiques sur le *darknet* et sur le web classique. Il commercialise des accès à Canal+, Disney+, Netflix, mais aussi à des comptes mails, des cartes de fidélités, 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 scrupule, Karys? 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 la source 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

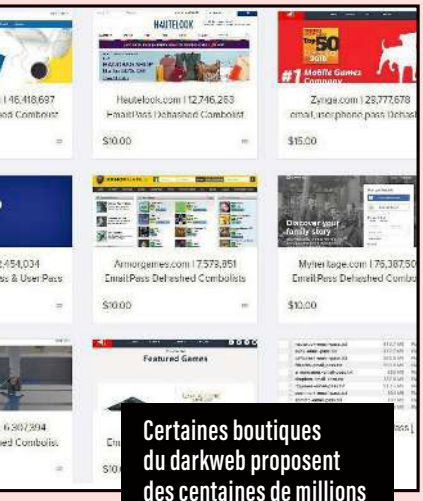
UNE FRAUDE BANCAIRE TOUTES LES 4 SECONDES

La double authentification (2FA) est une solution pour contrer les pirates. L'un d'eux a réussi à récupérer votre code d'accès à votre boutique préférée ou votre messagerie? Sans la seconde clé (2FA), il ne pourra arriver au reste de vos informations. Par ailleurs, il est fortement recommandé d'utiliser une adresse électronique et un mot de passe différent pour chaque site auquel on est abonné.

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 pouvant contenir des milliers de clients. Il suffit que j'y retrouve des adresses électroniques, des mots de passe, des numéros de téléphone. J'aurai toujours des acheteurs rien que pour ces trois données»,* explique le forban du Net. 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 forums où il était abonné.»* En d'autres termes, pour éviter de voir ses accès volés, mieux vaut ne pas suivre l'exemple de cet internaute imprudent. D'autant que cela semble être l'une des meilleures armes pour combattre les pirates.

Données médicales vendues à la pièce

Certains malfaiteurs vont encore plus loin et se moquent éperdument des conséquences de leurs agissements pour les particuliers et les sociétés dont les datas ont été exfiltrées. Leur credo ? Tant pis pour eux ! Tout se vend, tout s'achète, même des informations médicales sensibles… En février 2021, pas moins de 500 000 patients de 28 laboratoires situés dans l'ouest de la France ont ainsi vu leurs données de santé subtilisées. Leur identité, celle de leur médecin traitant, leurs pathologies, leur numéro de Sécurité sociale… tout s'est retrouvé en vente sur le darknet ! Comme le révélait le quotidien *Ouest France* dans un article publié le 13 décembre 2022, deux ans après, les victimes en subissent toujours les conséquences. Quotidiennement ciblées par des messages et des appels louches, elles vivent désormais dans la crainte d'arnaques et de vols et sont obligées de se méfier de tout.
D'autres malfaiteurs proposent à la vente des informations de santé dérobées à des hôpitaux ou des cliniques privées. Un exemple récent : celui du Groupement hospitalier de territoire (GHT) Cœur Grand Est, victime d'une cyberattaque en 2022. Les pirates du réseau criminel Industrial Spy lui ont réclamé 1,17 million d'euros pour que les milliers de fichiers volés ne soient pas diffusés sur Internet. La rançon n'a pas été payée. Depuis, les hackers commercialisent, dossier par dossier, l'ensemble du butin dérobé. Des passeports, des documents administratifs, des pièces d'identité sont vendus 3,60 € l'unité ! ■



Certaines boutiques du darkweb proposent des centaines de millions de données piratées.

Le site pirate Industrial Spy regorge d'informations volées.

COMMENT RÉAGIR SI L'ON EST VICTIME ?

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.

Escroquerie à l'amour, arnaque à la cryptomonnaie ou aux placements en Bourse, mais aussi virement frauduleux, fausse petite annonce, tentative de phishing… Les menaces sur la Toile sont nombreuses. Mais pas beaucoup plus que dans notre vie quotidienne, en fait ! La différence c'est qu'en ligne, les attaques sont plus concentrées et plus rapides, à cause des multiples connexions qui émaillent nos existences à l'heure du tout-numérique.

Que risquent 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 (par l'intermédiaire du phishing, par exemple), la loi considère cette action comme un moyen frauduleux, déloyal 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'identités, qui sont légion, les malfrats encourent une peine moins lourde: un an d'emprisonnement et 15 000 € d'amende (art. 226-4-1 du code précité).

N'hésitez jamais à dénoncer une arnaque que vous avez subie.

PIXEL-SHOT/ADOBE STOCK

Pas question de baisser les bras

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 décembre 2022, à l'issue d'une enquête de plusieurs mois, trois filous ont été arrêtés après avoir volé un Corrézien de 85 ans, qui avait eu le réflexe d'alerter la police. Grâce à un faux courriel imitant ceux de la banque de la victime, ils avaient pu accéder à son compte bancaire. Ayant relevé au maximum son autorisation de découvert, ils avaient effectué des virements à hauteur de 23 000 €.

Des adresses à connaître

C'est à juste titre que les autorités encouragent les victimes à dénoncer les faits délictueux en ligne. Il existe plusieurs sites dédiés aux plaintes à la suite

Les faux sites policiers existent également (lire aussi p. 70) ! Choisissez bien une plateforme officielle pour déposer plainte.

d'actes malveillants commis sur Internet. Même si la plupart de ces services publics (gratuits) n'autorisent que des signalements, ils s'avèrent utiles.

> **Pré-plainte en ligne** [1] a été mis en place par le ministère de l'Intérieur. Mais si ce site fait gagner du temps, il ne dispense pas d'une visite physique au commissariat ou à la gendarmerie pour l'enregistrement de la plainte. Il est avant tout conçu pour déclarer une atteinte aux biens (par exemple, un vol, une dégradation ou une escroquerie) dont vous êtes la victime directe, et dont l'auteur reste encore inconnu.

> **Perceval** s'adresse aux personnes ayant subi une ou des fraudes à la carte bancaire. Accessible via FranceConnect [2], la plateforme permet de faire un signalement en 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 les propos ou des comportements illégaux sur Internet [3]. On peut y signaler des faits de pédophilie, de racisme, d'incitation à la haine ou encore d'apologie du terrorisme.

> **Le dispositif Thésée** [4] permet de déposer une plainte, dans certains cas, ou de signaler une infraction relevant de la cybercriminalité (sites d'e-commerce malveillants, faux courriels, relations virtuelles malintentionnées…).

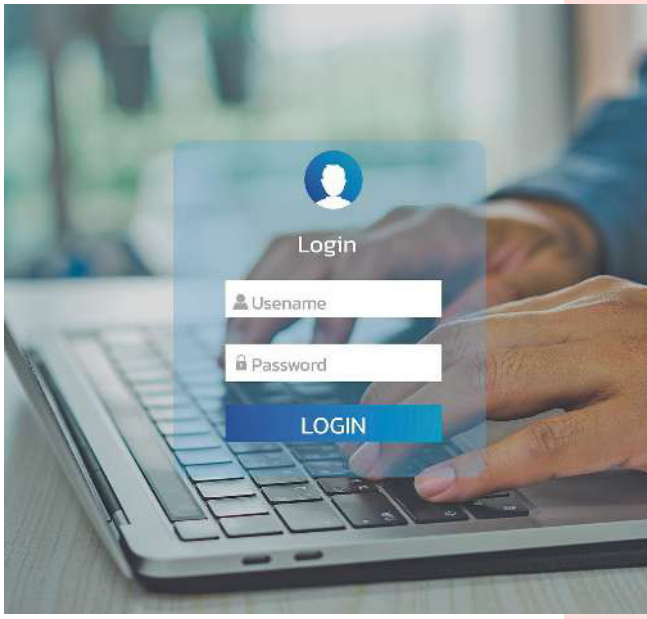
> **Ma Sécurité** [5] est un site officiel utile aux citoyens pour retrouver toutes les informations relatives à leur sécurité : annuaire des commissariats ou des gendarmeries, fiches pratiques sur les arnaques en ligne, etc. Avec cet outil, la gendarmerie nationale et la police accompagnent également les victimes dans leurs démarches après coup (préplainte, signalement de fraude, etc.). Enfin, il est également possible d'y échanger en direct, via un espace de discussion en ligne, avec un gendarme ou un policier.

Bon à savoir Le démarchage commercial des titulaires d'un compte personnel de formation (CPF) est interdit depuis le 1er janvier 2023. Cette mesure a été prise pour lutter contre les arnaques au CPF, très nombreuses ces derniers temps. Toute prospection par téléphone, SMS, courriel ou réseaux sociaux auprès des bénéficiaires de ce dispositif est prohibée. Le manquement à cette interdiction est passible d'une amende administrative de 75 000 € pour une personne physique et de 375 000 € pour une personne morale. ■

(1) Pre-plainte-en-ligne.gouv.fr.
(2) Service-public.fr/particuliers/vosdroits/R46526.
(3) Internet-signalement.gouv.fr.
(4) Service-public.fr/particuliers/vosdroits/N31138.
(5) Masecurite.interieur.gouv.fr.

MOTS DE PASSE LAISSEZ FAIRE LE GESTIONNAIRE !

Retenir tous les mots de passe, quelle galère… Et si vous les confiez à un logiciel spécialisé ? Nous en avons testé 12, la plupart sont efficaces.



La gestion quotidienne de vos identifiants vaut bien d'y consacrer quelques euros par mois. Qui ne peste pas à chaque fois qu'il faut créer ou se souvenir d'un mot de passe ? Vous utilisez toujours le même pour vous simplifier la vie ? Grave erreur ! Si quelqu'un tombe dessus, vous lui offrez l'accès à tous vos comptes. Vous alternez entre « 123456 » et « 654321 » ? Inconscience ! Les suites logiques, de chiffres mais aussi de lettres ou de mots, sont parmi les plus simples à deviner. Vous variez les mots de passe, mais les consignez dans un dossier sur votre bureau pour les avoir sous la main ? C'est déjà un pas… qui reste insuffisant : un document bureautique, même verrouillé par un mot de passe (encore un), est facile à « craquer » (lire aussi p. 42).

Plusieurs atouts, mais une contrainte

Avec nos vies numériques, entre les achats sur Internet, les impôts en ligne, les factures dématérialisées, les comptes retraite, formation et autres, administrer ses mots de passe est devenu un enfer. Heureusement, des outils spécialisés sont là pour nous y aider. Ces logiciels payants (les versions gratuites sont limitées à 14 ou 30 jours, ou bien à un seul accès) ont tout prévu : ils suggèrent des mots de passe robustes lorsqu'il faut en créer un sur des sites, les enregistrent puis remplissent automatiquement les cases quand vous vous connectez. Tous (sauf Trend Micro Password Manager) proposent d'importer les mots de passe que vous stockiez dans votre navigateur, et tous vous alertent quand ils sont trop faibles. Ils peuvent aussi gérer les identifiants de plusieurs utilisateurs sur un même site, voire autoriser l'accès d'un compte à l'un de vos proches sans lui révéler le fameux sésame. Leur seule contrainte : ils ne s'ouvrent qu'avec un mot de passe « maître », que vous définissez au départ. Ce dernier doit être complexe, composé de chiffres, de lettres et de caractères spéciaux, et il ne faut jamais l'oublier. Sans lui, tous les autres seront perdus… Et impossible de le récupérer, car l'éditeur ne le stocke pas.

Autre bémol : la configuration de ces gestionnaires prend un peu de temps et, globalement, leur ergonomie s'avère moins bonne sur un smartphone que sur un ordinateur. Même le meilleur, Dashlane Advanced (retrouvez le guide d'installation p. 64), ne permet pas d'importer des mots de passe stockés dans un téléphone… Sachez toutefois que certains offrent des fonctions annexes, comme la sauvegarde de documents personnels dans le cloud. Pour autant, si vous avez besoin d'un espace de stockage conséquent, nous vous conseillons plutôt de recourir à un logiciel en ligne dédié (lire aussi p. 36).

KHUNKORN/ADOBE STOCK

Test

12 SOLUTIONS PAYANTES

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

		Utilisation											
		Ordinateur			Smartphone								
		ACHAT/INSTALLATION	CONFIGURATION	UTILISATION COURANTE	IOS	ANDROID	SÉCURITÉ	FONCTIONNALITÉS	APPRÉCIATION GLOBALE		PRIX LICENCE	STOCKAGE DE DOCUMENTS PERSONNELS	CONNEXION D'UN TIERS SANS MOT DE PASSE
									Note sur 20		€/an		
1	**DASHLANE** ADVANCED	★★★	★★	★★	★	★	★★	★★★	**14,6**	★★	33	●	-
2	**ROBOFORM** EVERYWHERE	★★★	★★	★★	★	★	★★	★★★	**14,5**	★★	22,34	-	●
3	**KEEPER** UNLIMITED PERSONNEL	★★★	★★	★★	★	★	■	★★★	**14,4**	★★	42	●	-
4	**1PASSWORD**	★★★	★	★★	★★	★	★★	★★★	**14,1**	★★	33,56	●	-
5	**NORDPASS** PREMIUM	★★★	★★	★★	★	★★	★★	★★	**13,7**	★★	32,28	-	●
6	**LASTPASS** PREMIUM	★★★	★★	★	★★	★	★★	★★★	**13,5**	★★	34,80	●	●
7	**ENPASS** INDIVIDUAL PLAN	★★★	★	★★	★★	★	★	★★	**13,4**	★★	21,49	●	-
8	**BITWARDEN** PREMIUM	★★	★	★	★★	★★	★★	★★★	**12,9**	★★	9,35	●	-
9	**STICKY PASSWORD** PREMIUM	★★★	★★	★	■	■	★★	★★	**12,1**	★★	29,95	-	-
10	**ZOHO** VAULT STANDARD	★	★	★★	■	■	★★	★★★	**11,8**	★	10,80	●	●
11	**F-SECURE** ID PROTECTION 5 APPAREILS	★★★	■	■	■	■■	★★	★★	**9**	★	49,99	-	-
12	**TREND MICRO** PASSWORD MANAGER	★	★	■	■	■	★★	★★	**9**	★	9,95	-	-

NOTRE MÉTHODE

Nous évaluons la facilité d'utilisation en achetant une licence (pour Windows et MacOS, Android et iOS), en configurant les logiciels (création du compte et du mot de passe maître, imports des identifiants du navigateur…) et en les utilisant au quotidien. Nous vérifions ensuite que les données sont bien protégées (force des mots de passe, biométrie, etc.) et que les fonctions attendues sont présentes.

Le meilleur

DASHLANE

Dashlane ADVANCED
33 €/an **14,6/20 | ★★**

Dashlane Advanced est facile à installer sur un PC ou un Mac (un peu moins sur un smartphone). Une page d'importation fournit des liens pour récupérer les identifiants de différentes sources (navigateurs web notamment). Capable d'enregistrer un nombre illimité de mots de passe, le logiciel offre de nombreuses autres fonctions (stockage de documents et des données bancaires pour payer en ligne, par exemple).

L'alternative

RoboForm

Roboform EVERYWHERE
22,34 €/an **14,5/20 | ★★**

Ce logiciel efficace s'avère plus ergonomique sur ordinateur que sur smartphone. Pas de problème pour l'achat (si ce n'est que toutes les instructions ne sont pas traduites), ni pour la configuration. Par défaut, les mots de passe générés comprennent 16 caractères, mais vous pouvez changer ce nombre (de 1 à… 512 caractères !). Il est aussi possible de partager ses accès avec des tiers sans livrer ses mots de passe.

Pas-à-pas

INSTALLER ET CONFIGURER DASHLANE

● **Objectif :** profiter des fonctionnalités d'un gestionnaire de mot de passe sur un ordinateur et sur un téléphone. ● **Niveau de difficulté :** assez facile. ● **Temps nécessaire :** 10 à 15 minutes.

Création du compte et du mot de passe maître

Ne sortez pas votre carte bancaire: Dashlane offre un mois d'essai gratuit, ce qui permet d'essayer le logiciel avant de s'abonner. Pour le faire fonctionner sur un ordinateur, une extension de navigateur est proposée (Chrome, Edge, Firefox ou autre). Une fois l'installation réalisée, l'outil vous invite à créer un compte, avec un e-mail et un mot de passe «maître». Ce dernier s'avère la seule donnée que Dashlane ne peut pas enregistrer. Comme il faudra le renseigner par vous-même à chaque connexion (image 1 p. 65), prenez votre temps pour en inventer un tranquillement. Un mot de passe doit être facile à mémoriser pour l'utilisateur, mais difficile à deviner pour un pirate (lire nos conseils en la matière p. 42). Attention, si vous l'oubliez, Dashlane, qui ne le connaît pas, ne pourra rien pour vous !

Importation des mots de passe existants

Si vous pouvez vous connecter à vos sites internet habituels sans qu'il soit nécessaire de taper des mots de passe, c'est que votre navigateur les a enregistrés. Il faudra donc les transférer dans Dashlane pour les stocker en sécurité. L'opération se déroule en deux temps: d'abord, ils doivent être «exportés» du navigateur, ce qui consiste à les enregistrer dans un petit fichier texte. Puis il faut les «importer» dans le coffre-fort du gestionnaire (images 2 et 3). La procédure d'exportation dépend de chaque navigateur, mais l'aide en ligne de Dashlane peut vous accompagner tout au long du processus (image 4). Celle d'importation est, quant à elle, très bien guidée.

Suppression des enregistrements

Par défaut, le logiciel bloque l'enregistrement des nouveaux mots de passe dans le navigateur. Mais il n'élimine pas ceux déjà sauvegardés ! Résultat, le navigateur comme Dashlane voudront tous les deux gérer la connexion à vos sites web… Pour éviter la confusion, nous vous conseillons d'ouvrir les options de stockage des mots de passe dans le navigateur et de tous les supprimer (image 5). De même qu'il ne doit y avoir qu'un seul capitaine sur un navire, il ne faut qu'un seul gestionnaire dans un ordinateur !

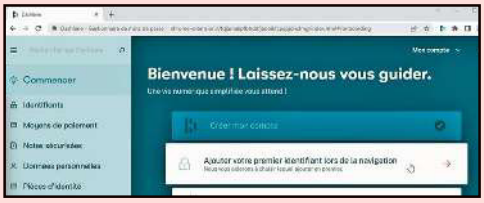
Remplacement du gestionnaire intégré

Sur les smartphones, Dashlane fonctionne avec n'importe quelle application, il ne se limite pas aux navigateurs internet. De fait, même si les téléphones bénéficient d'un gestionnaire de mots de passe intégré (Keychain sur iPhone, et généralement Google pour Android), Dashlane peut s'y substituer (images 6 et 7). C'est alors lui qui affichera des propositions d'identifiants ou de mots de passe lors d'une connexion.

Par **Patrick Gérard** (HC Lab)

Les étapes essentielles

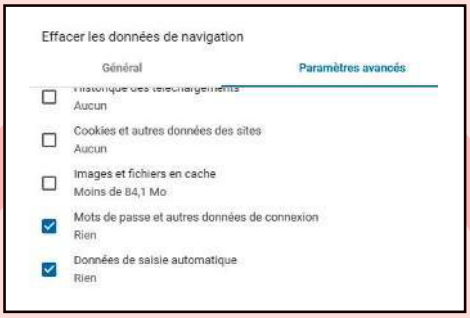
1 La création du mot de passe « maître » (celui ouvrant Dashlane) est une étape cruciale. Nous vous suggérons de le mettre au point en amont et de le vérifier en cliquant sur l'icône « œil ».



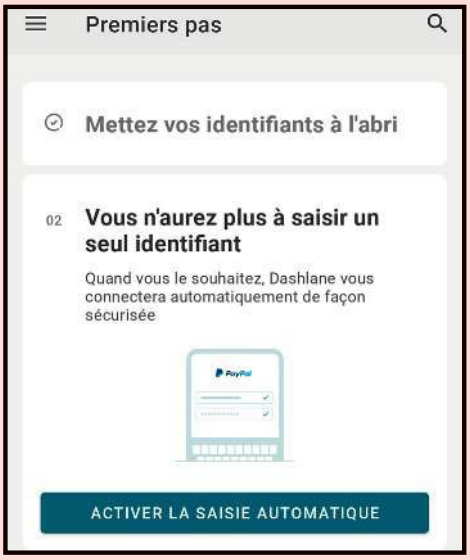
2 Lors de la connexion initiale (ou avec l'option « Commencer »), Dashlane vous invite à enregistrer votre premier identifiant.

3 Plutôt que de les renseigner un à un, on choisira « Importer plusieurs identifiants à la fois » en cliquant sur le bouton « Importer ».

4 En fonction de la source de vos identifiants, Dashlane vous indiquera la procédure à suivre, avec des liens vers les aides en ligne.



5 Une fois les mots de passe importés, il est préférable de les supprimer du navigateur, un par un ou via les options de confidentialité, comme ici dans Google Chrome.



6 À peine installé sur un téléphone, Dashlane propose de s'activer pour toutes les applications, en remplacement du gestionnaire d'identifiants déjà en place.

7 Cette option présente les gestionnaires d'identifiants possibles (ici, sur un téléphone Android). Il suffit de sélectionner Dashlane.

DONS D'ANIMAUX : LES FRAUDES SE MULTIPLIENT

Vous avez repéré une petite annonce proposant le don d'un chiot ou d'un chaton ? Attention, en craquant pour l'adorable boule de poils sur la photo, vous risquez de vous jeter dans la gueule du loup !

Les cybercriminels ont une méthode simple: ils publient des petites annonces sur des sites gratuits. Ils prétendent qu'ils doivent donner leur compagnon à quatre pattes en raison d'un départ en maison de retraite ou d'un déménagement, que leur chienne a eu des petits dont ils ne peuvent s'occuper, etc. 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 payer les frais de transport. Parfois, ils 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 !

Prenez le temps de lire attentivement l'annonce et vérifiez les détails : la photo du chat à donner se trouve-t-elle ailleurs sur Internet ?

Gare aux cartes bancaires prépayées

En général, les fraudeurs réclament un paiement 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 paiement du transport,* explique un escroc, *vous devez acheter deux coupons physiques d'une valeur de 150 €. »* Il est possible d'acquérir ces derniers auprès de sites spécialisés ou d'un buraliste, de façon tout à fait légale et très courante. Vous versez la somme sur la carte/ticket puis fournissez le code de la transaction à la personne que vous devez payer. Grâce à ce numéro, l'arnaqueur touche le montant convenu… et disparaît dans la nature. Autre méthode criminelle souvent utilisée: le faux site de société 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 escrocs n'hésitent pas à répondre à l'appel afin de convaincre leur correspondant.

Peu après la confirmation, par le «donateur» de l'expédition de l'animal, la personne qui souhaite l'adopter est contactée, soit par un faux vétérinaire, soit par la société de transport bidon. On lui indique 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, une cage appropriée est à acheter. C'est ici que les voyous plument leurs victimes. Des sommes qui peuvent atteindre plusieurs centaines d'euros pour les plus crédules.

Pas de précipitation

Pour 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 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 ou par carte prépayée ou carte-cadeau. Surtout, n'envoyez jamais d'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 !

Adopter des solutions plus sûres

Si vous souhaitez avoir un animal de compagnie, il existe d'autres façons de l'acquérir que les petites annonces du Web. Elles sont en général plus sûres. La première est de s'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-dessous). Cette option a le mérite de permettre 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 (famille, amis, 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 les sites La-spa.fr ou Lpa-nf.fr. ■

COMMENT RÉAGIR EN CAS D'ARNAQUE

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 une amende de 375 000 € ou une peine d'emprisonnement pouvant atteindre cinq ans.

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

N. JACOBI/ISTOCK ; J.-C. MOSCHETTI/REA

OUPS, VOUS AVEZ ÉTÉ PIRATÉ !

Voici l'histoire complètement folle d'Angélique. Cette Parisienne a dû faire face au piratage de son compte dédié à l'administration fiscale.

Angélique (nous avons modifié son prénom) a une trentaine d'années. Cette jeune femme est une professionnelle de la communication. Elle utilise chaque jour des adresses électroniques, surfe sur Internet, transfert et télécharge de nombreux fichiers plus ou moins sensibles (factures, etc.). En 2022, elle reçoit un message de l'administration fiscale l'informant du versement de plusieurs milliers d'euros correspondant à un crédit d'impôt auquel elle aurait droit. «*J'avoue mon étonnement,* raconte-t-elle, *d'autant que l'on m'indique des remboursements liés à une garde d'enfant et à des travaux de jardinage. Seul problème, je n'ai jamais déclaré de dépenses de ce type.*» Ni une ni deux, Angélique alerte le fisc et explique son cas. «*Ils ont été très rapides et compréhensifs. Ils m'ont rassurée. Je ne serai pas dans l'obligation de rembourser cette somme que je n'ai pas perçue !*»

Le pirate a rectifié la déclaration fiscale pour toucher des crédits d'impôts...

LE DROIT À L'ERREUR, UNE AUBAINE

L'escroc a détourné le dispositif des réductions d'impôt à son profit en manipulant le compte de contribuable d'Angélique. Quand on sait que pour un emploi à domicile, par exemple, le crédit d'impôt correspond à 50% des dépenses engagées sur l'année par un particulier, on comprend l'intérêt de ce piratage. La première action du malfaiteur a été de mettre la main sur les informations personnelles d'Angélique. Notamment son numéro fiscal, qui permet d'accéder à son compte sur Impots.gouv.fr. Mais le site est bien sécurisé: pour s'y connecter, on doit employer un mot de passe ou, mieux encore, la plateforme d'identification FranceConnect. Le pirate a donc trouvé un autre moyen. «*Je pense qu'il a collecté mes informations via des dossiers que j'ai communiqués par courriel alors que je recherchais une location à Paris*», souligne Angélique.

Le malfaiteur a ensuite exploité Oups.gouv.fr, mis en place par la loi pour un État au service d'une société de confiance (Essoc). Avec Oups, tout citoyen a le droit de se tromper dans une déclaration. Quand cela arrive, l'administration corrige ses données et ne le sanctionne pas s'il s'agit de la première fois. «*Le pirate a fait rectifier ma déclaration de revenus en rajoutant des prestations d'aide à domicile*», commente Angélique. Après, il lui a suffi d'attendre le versement du crédit d'impôt en ayant pris soin, en amont, de faire modifier aussi l'adresse postale d'Angélique, afin de recevoir le chèque du Trésor. Terriblement efficace !

M. GAILLARD/REA PIXEL ; SHOT/ADOBE STOCK

COMMENT SE PROTÉGER ?

La mésaventure d'Angélique peut arriver à n'importe qui. La fuite de données personnelles est malheureusement à prendre en compte dans la vie de tous les jours. Vous devez fournir des documents administratifs ? 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). Angélique a fourni, lors de sa recherche de logement, de nombreuses photocopies de documents exploitables par un escroc, comme l'avis d'imposition sur lequel figurait son numéro fiscal. Du pain béni pour un faux bailleur !

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 de réaliser 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 neuf partenaires d'identification proposés, tels que La Poste, l'Assurance maladie (Ameli) ou encore Impots.gouv.fr. Lors de la première utilisation, vous devrez 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…

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

L'usage de FranceConnect présente toutefois quelques inconvénients potentiels. Tout d'abord, certaines personnes peuvent être réticentes à partager leurs informations personnelles 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 un utile pour qui souhaite réaliser des démarches administratives en ligne en toute sécurité. Depuis sa mésaventure, Angélique l'utilise ! ■

LA DOUBLE PEINE AVEC LES FAUX POLICIERS

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

Jeanine a 67 ans. Heureuse dans la vie, elle est amatrice de jolis objets qu'elle déniche dans des brocantes ou des marchés aux puces sur Internet. Sauf qu'en ce mois de mai 2022, un flacon en verre du XVIIIe 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. L'amatrice d'art saute sur l'occasion et prend contact avec cette dernière. «*La dame au bout du fil était avenante, connaissait son sujet,* souligne la collectionneuse. *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'affaire aurait pu s'arrêter là, mais 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 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 % de la somme volée… Eh bien savez-vous ce qu'a fait Jeanine ? «*J'avoue être un peu honteuse ! J'ai été roulée une seconde fois. J'ai réglé les frais demandés, sans même me poser de question. J'ai pu me dire que cela était onéreux, mais*

L'AMF NE RESTITUE PAS D'ARGENT

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-le, tout comme la police, l'AMF n'est pas habilitée à restituer des sommes perdues par des épargnants.

Une victime n'a pas intérêt à chercher de l'aide en ligne. Se rendre au commissariat est bien plus sûr.

j'étais si heureuse de récupérer mes fonds !» Bilan, Jeanine a perdu 1 320 € au total. Le plus terrible dans cette histoire est que l'escroc au féminin et le faux policier ne se connaissent pas… 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 appelle et se présente comme un policier capable de vous faire récupérer votre argent, raccrochez sans hésiter.

Méfiance sur les espaces de discussion publics

Les escrocs sont aussi très présents sur les blogs et les forums. Leur méthode est simple: ils diffusent de faux témoignages. Un 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, pour 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 gendarmerie, Interpol ou encore Europol. Nous sommes notamment tombés sur Services-paiements-amendes.fr ; Amendes-gouvernement.fr ; Amendes-payer.fr ; Paiement-contravention.fr ; Bot-interpol.fr ; Europol-ministere-interieur.fr. Soyez vigilant !

ÉRIC TSCHAEN/REA ; P. TURPIN/PHOTONONSTOP

CES MAÎTRES CHANTEURS VIRTUOSES DE LA PEUR…

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

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. Mais le pirate «rassure» en affirmant oublier ces images contre quelques centaines d'euros… Ça semble gros, mais des milliers de personnes ont payé. En réalité, le pirate n'avait jamais eu accès à leurs machines, il n'a fait que joué sur la peur du «qu'en-dira-t-on». Depuis six ans, des arnaques de ce type réapparaissent régulièrement. Les malfrats utilisent les adresses électroniques qu'ils ont pu récupérer sur des sites, des forums, etc. En 2019, 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.

L'escroquerie à la webcam peut se produire sans que l'on en soit conscient.

Mauvais film

Il est possible de se faire piéger via une caméra connectée. Les rendez-vous amoureux devant une webcam, par exemple, peuvent 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, 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 aussi sans que la victime en soit même consciente. Des logiciels en apparence légitime, 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.

La vigilance est de mise

Il existe plusieurs mesures pour vous protéger. D'abord, restez vigilant lorsque 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 demeurera audible). Enfin, il est fortement recommandé de ne jamais partager d'informations confidentielles en ligne, filmées ou non. ■

ARTPOST - STOCK.ADOBE.COM ; IDOLFOTO/ADOBE STOCK

ON VOUS FAIT LE COUP DE LA PANNE

Vous surfez sur le Web, quand soudain une fenêtre vous annonce que votre ordinateur est piégé. Le téléphone d'un « service technique » s'affiche…

L'arnaque au faux service technique est courante. Vous êtes sur Internet, quand tout à coup des fenêtres d'alertes surgissent. 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…

Un appel qui va coûter cher

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…

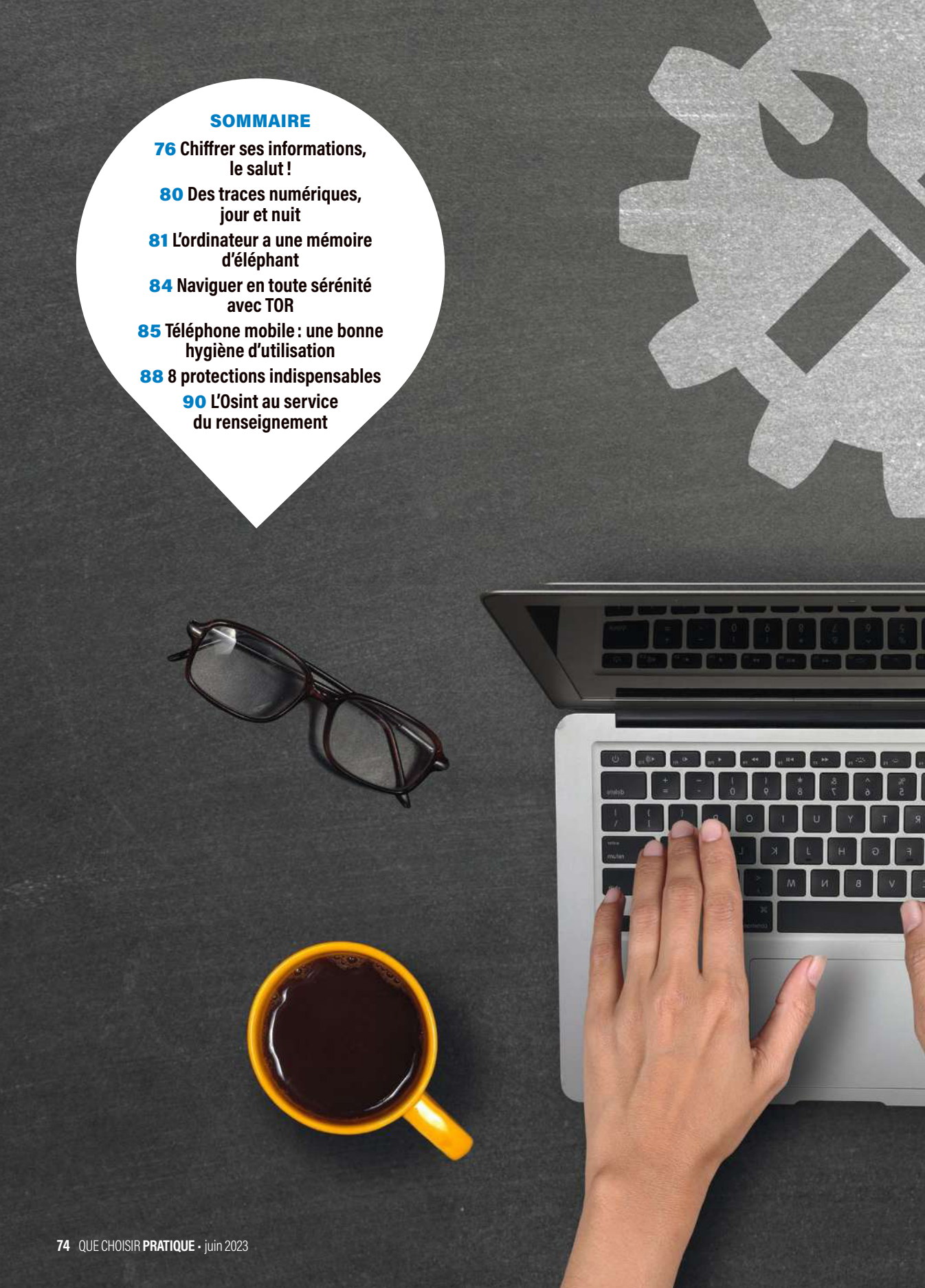
L'ordinateur est fouillé

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 données 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 ordinateur. 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 simultanément sur les touches Ctrl, Maj et Q. 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-le 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.

SOMMAIRE



Les bons outils

Dans ce chapitre, nous verrons qu'il est fondamental de bien s'équiper pour naviguer sereinement. Sans logiciels dédiés à la protection de la vie privée, les risques sont grands de voir ses données personnelles finir entre les mains de pirates. Investir dans la cybersécurité est essentiel, car dans notre monde connecté, nos machines présentent des vulnérabilités alors que les menaces en ligne ne cessent de s'étoffer.
Si certaines solutions de protection (antivirus, pare-feu…) s'avèrent coûteuses, d'autres sont gratuites. Nous vous présentons ici les meilleures du marché, assorties de quelques conseils utiles pour vous prémunir des dangers au quotidien. Mais rappelons que si « les bons outils font les bons ouvriers », les miracles, eux, n'existent pas : la sûreté de l'environnement numérique dépendra toujours et avant tout de l'attitude de l'internaute…

TRILOKS/ISTOCK

CHIFFRER SES INFORMATIONS, LE SALUT !

Pour éviter que des documents numériques soient consultés par des personnes non autorisées, une solution existe : le chiffrement.

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 peut toucher tout le monde, même les plus 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 (lire l'encadré ci-dessous). Bref, aujourd'hui, les besoins de protection s'avèrent de plus en plus importants.

ALPHASPIRIT/ADOBE STOCK

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 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 peuvent rester secrètes, notamment celles en ligne. En effet, sécuriser des informations circulant sur la Toile commence par le chiffrement des échanges entre internautes et 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 signifient en effet que la communication est chiffrée.

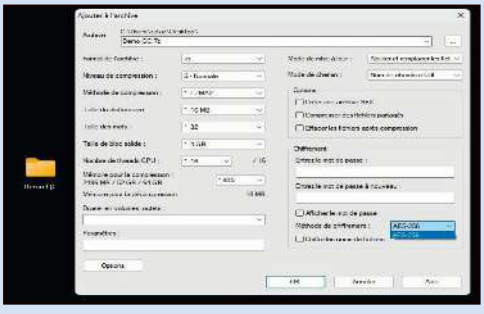
INTERCEPTION EN PLEINE RUE

Paris, février 2023. La police découvre une étrange valise raccordée à des antennes à l'arrière d'une voiture. Il s'agit d'un IMSI-Catcher, un dispositif normalement utilisé par les services secrets pour intercepter des connexions de téléphones portables. Mais là, des pirates profitaient des mobiles des passants pour envoyer des SMS usurpateurs !

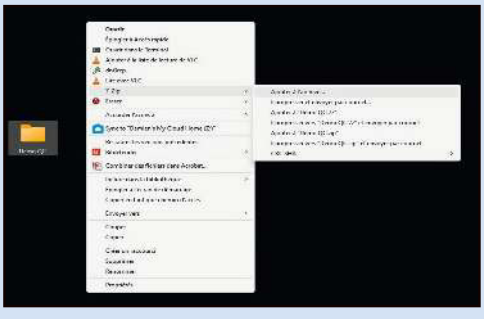
CRÉER UN CONTENEUR AVEC 7-ZIP

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.

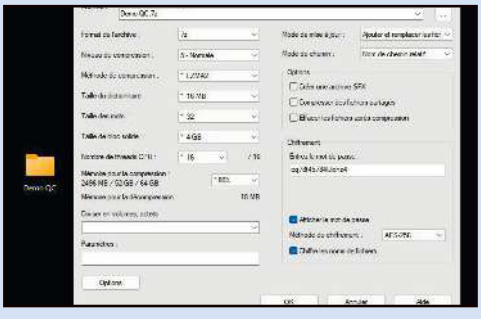
1 Installer 7-zip sur son ordinateur.



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



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



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

Dès lors, les conversations (par tchat, messagerie, etc.) entre l'émetteur et le récepteur ne peuvent être ni écoutées ni interceptées.

Chiffrer ou crypter ?

On entend parfois des personnes dirent «*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 (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). De fait, 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» ou «désencrypter» (il s'agit d'anglicismes), mais «déchiffrer» (par exemple, un texte, 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, chiffrer et crypter.

S’initier à la substitution

De nombreuses solutions (payantes et gratuites) permettent de se lancer dans le chiffrement, mais toutes ne sont pas simples à exploiter pour des novices. Nous allons donc nous attarder sur les logiciels gratuits et faciles d’accès. En guise d’introduction, découvrons une méthode de chiffrement vieille comme le monde (et donc, pas 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, la lettre A devient D, la lettre 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 et disques durs (lire l’encadré p. 79). 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 le disque dur de 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.

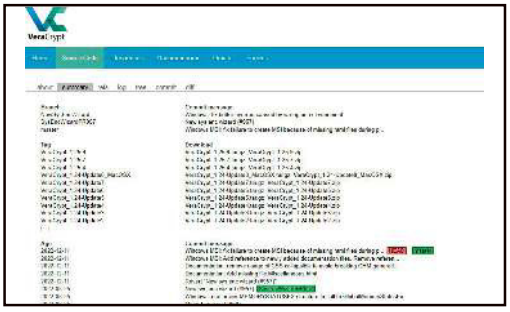
PROTON MAIL

Ce service de messagerie garantit la confidentialité des mails. Les messages envoyés et reçus via ce dispositif sont chiffrés de bout en bout. 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.

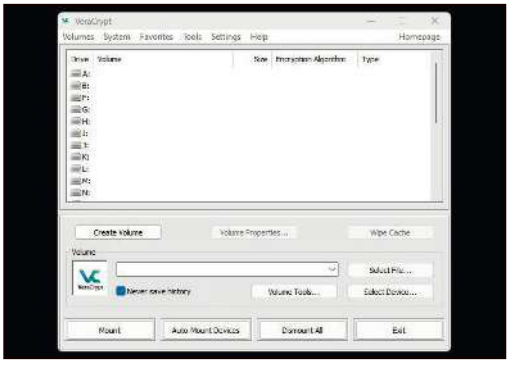
Fiche pratique

CHIFFRER AVEC VERACRYPT

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



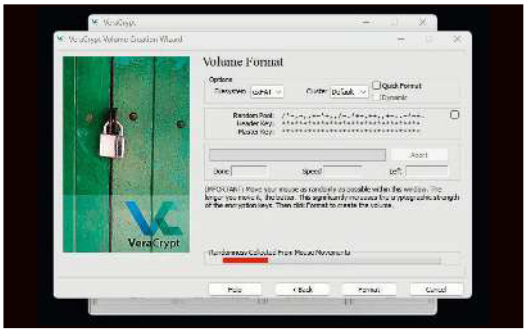
1 Télécharger le logiciel depuis le site Veracrypt.fr et l'installer sur son ordinateur ; l'ouvrir.



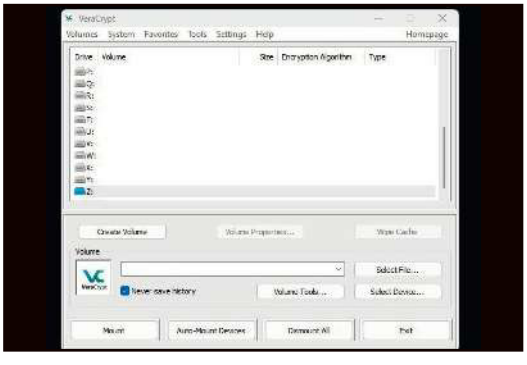
2 Sélectionner *Create Volume* (« Créer un volume »), puis *Create an encrypted file container* (« Créer un fichier conteneur chiffré »). Cliquer sur *Next* (« Suivant »), choisir l'endroit où enregistrer le document et le nommer.

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. On peut y stocker ses documents sensibles en toute sécurité.



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

DES TRACES NUMÉRIQUES, JOUR ET NUIT

Un ordinateur allumé laisse des empreintes. Comme elles peuvent être collectées et utilisées à diverses fins, il faut savoir les effacer.

Les traces numériques les plus courantes laissées par les appareils informatiques incluent les journaux d'activité, les fichiers temporaires, les cookies, les historiques de navigation et les fichiers de sauvegarde. Autant d'informations qu'il faut pouvoir maîtriser et détruire si nécessaire, par exemple quand on veut revendre ses machines.

Pourquoi faire le ménage ?

Ce que l'on stocke sur son ordinateur privé peut être extrêmement sensible (informations personnelles ou financières, mots de passe, fichiers professionnels qui ne devraient pas s'y trouver…). Supprimer des documents en les déposant simplement dans la poubelle n'est pas suffisant, car un logiciel de récupération de données pourrait les faire ressurgir. En réalité, des informations ne sont réellement éradiquées que lorsqu'elles sont écrasées par de nouvelles.

Supprimer définitivement les traces

La plupart des systèmes d'exploitation modernes, tels que Windows et MacOS, possèdent une option de suppression sécurisée. Les informations sont broyées par des zéros ou des uns, ce qui rend leur récupération pratiquement impossible. Voici comment s'y prendre:

• **Sur Windows:** faire un clic droit sur le fichier ciblé et sélectionner «Supprimer». Ensuite, maintenir la touche Maj enfoncée et cliquer à nouveau sur «Supprimer»; une boîte de dialogue demande alors de confirmer la suppression du fichier.

• **Sur Mac:** après un clic droit sur l'élément visé, on sélectionne «Déplacer vers la corbeille» dans le menu. Ensuite, on maintient la touche Option enfoncée et on clique sur «Vider la corbeille»; cela éradique les fichiers de façon définitive. L'effacement peut aussi passer par des logiciels basés sur des algorithmes spéciaux. Leur objectif: comprimer les données plusieurs fois pour rendre la récupération quasi impossible. Les plus populaires se nomment Eraser, CCleaner (lire les encadrés p. 82) ou encore Darik's Boot and Nuke. Attention ! S'ils sont simples d'utilisation, ces outils s'avèrent aussi très puissants: on s'assurera donc de ne pas se tromper de support (disque dur, clé USB, etc.) avant de les lancer, car les éléments seront ensuite totalement effacés.

Veillez à ce que personne ne s'empare de vos données.

D. ANDISON/ADOBE STOCK

Gare à vos équipements connectés !

Saviez-vous que le routeur, ce boîtier que vous avez acheté pour partager votre connexion internet dans toute la maison, stocke de nombreuses informations sensibles? En avril 2023, le laboratoire Eset a découvert que sur 16 routeurs vendus en seconde main, 9 contenaient des données privées et personnelles… Soyez donc vigilant ! ■

L'ORDINATEUR A UNE MÉMOIRE D'ÉLÉPHANT

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

Une machine est ainsi programmée: elle collecte constamment des données (nom, 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'erreur, 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.

Rôle de 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», en français), 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 donc, dans leur Mac, d'une «mémoire virtuelle», sécurisée et préconfigurée. 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 >>

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».

EFFACER SES TRACES AVEC CCLEANER

L'application CCleaner (Ccleaner.com), 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 : CCleaner fera le ménage.

>> 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 peuvent être employées pour suivre ses activités. Il est donc important de prendre des mesures de protection, comme l'effacement régulier des fichiers temporaires (dans Windows, il s'agit du répertoire Temp) et des cookies (lire l'encadré p. 81). 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 et de son imprimante, date des impressions, logiciels mis en œuvre, etc.). Les logs sont gardés dans un ordinateur sans limite de temps… Des logiciels tels que CCleaner (lire l'encadré p. 82) ou Wise Disk Cleaner peuvent les faire disparaître, mais il faut quand même rester prudent, car ils ont leur utilité. Ils permettent en effet à la machine de ne pas rencontrer une erreur une seconde fois et lui éviter de se bloquer.

Des outils de surveillance bien utiles

Deux outils gratuits permettent de contrôler l'activité de son ordinateur: ActivTrak et Time Doctor. Ils proposent des fonctionnalités comme

DÉTRUIRE 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. En fonction de 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.**

ADOBE STOCK

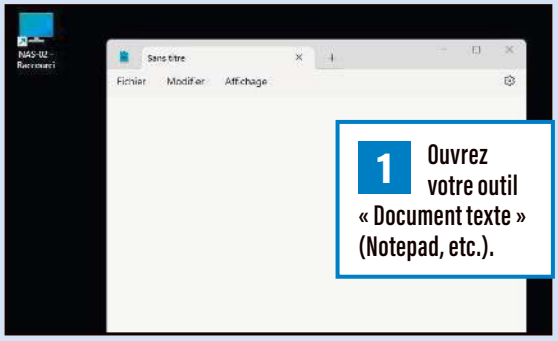
la capture d'écran et la surveillance des applications et des sites web visités. Une fois installés, ces logiciels enregistrent ces données et les stockent… dans les clouds (espaces nuagiques) des deux sociétés qui les éditent. Il faudra par conséquent se rendre sur Activtrak.com ou Timedoctor.com pour les consulter.

Les logiciels ont eux-mêmes de la mémoire

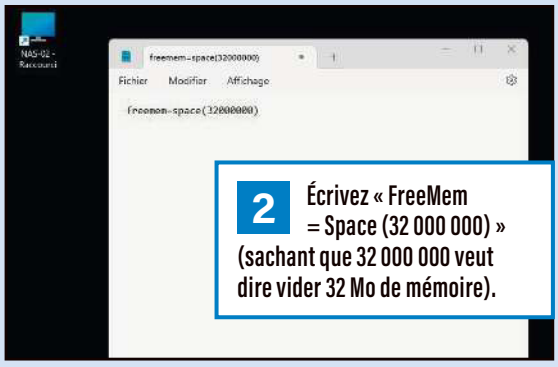
Un ordinateur sauvegarde énormément d'informations sur les activités de son propriétaire, mais il n'est pas le seul. Les logiciels de travail – traitement de texte, gestionnaire d'image, navigateur et imprimante, pour ne citer qu'eux – collectent également des tonnes de renseignements. Or, ils créent 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 de formats, ou 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, si le cliché a été pris avec un smartphone, sa géolocalisation. 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

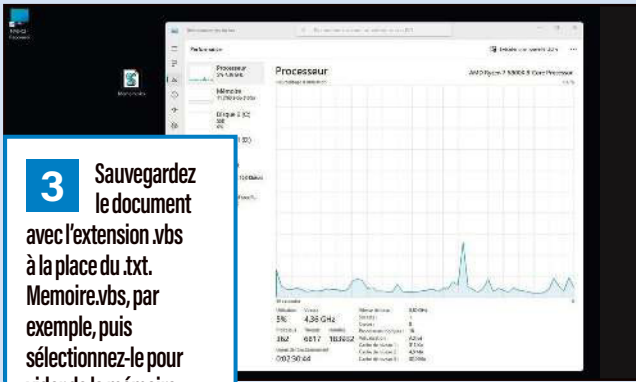
Avant de fermer votre ordinateur, ouvrez plusieurs images à l'écran. Leur poids écrasera les informations que la mémoire vive a pu collecter. Autre méthode, plus geek : créez un petit fichier sur votre bureau (code ci-dessous) et exécutez-le quand bon vous semble. Des logiciels gratuits comme Wize Memomy 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 (32 000 000) » (sachant que 32 000 000 veut dire vider 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.

NAVIGUER EN TOUTE SÉRÉNITÉ AVEC TOR

Vous souhaitez surfer d'une manière anonyme, sans laisser de traces ni de quoi vous géolocaliser ? Le navigateur TOR devrait vous y aider.

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 et sa géolocalisation. Quand vous le visitez, il ne sait pas qui vous êtes et 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.

Adresses simples et complexes

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. Il 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 (comme Ufc.quechoisir.org), ou se terminant par .onion (comme pour le moteur de recherche DuckDuckGo, Duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion). Ces dernières adresses 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. Et 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.

TOR vous relie au site souhaité grâce à plusieurs machines disséminées dans le monde entier.

TOR, sécurisé à 100 % ?

Il faut noter que le navigateur TOR ne garantit pas l'anonymat de l'ensemble des connexions internet de l'ordinateur: seules celles établies par son truchement sont anonymisées. Toutes les autres – lorsque vous vous connectez à une messagerie par exemple, ou que vous passez par d'autres navigateurs web (Chrome, Edge, etc.) – ne le sont pas. De plus, bien que TOR minimise les traces numériques laissées, certaines peuvent toujours être enregistrées sur le disque dur de la machine, comme les cookies, l'historique de navigation, les fichiers téléchargés ou les marque-pages. ■

KERMALO/REA ; SUPATMAN/ADOBE STOCK

TÉLÉPHONE MOBILE : UNE BONNE HYGIÈNE NUMÉRIQUE

Protéger ses données personnelles sur son portable est primordial. Voici quelques 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. L'option schéma de déverrouillage n'est, elle, pas recommandée, car elle est plus facile à intercepter par un individu regardant l'utilisateur le dessiner.

Les mises à jour du téléphone, de son système d'exploitation et de ses applications sont aussi capitales pour la sécurité. Il ne faut pas les remettre à plus tard, car elles colmatent de potentielles portes d'entrée pour les pirates. Par ailleurs, activer l'option «Localiser mon appareil» est utile pour retrouver son smartphone en cas de perte ou de vol, mais aussi pour détruire son contenu et/ou empêcher son utilisation.

On ne le répétera jamais assez, mais se connecter à des wifi publics non sécurisés (proposés par des hôtels, des restaurants…) est dangereux. Ces connexions sont vulnérables aux attaques de malveillants qui, eux aussi, se connectent. Quand on n'a pas d'autre choix que de s'y raccorder, il faut utiliser un réseau privé virtuel (VPN) pour sécuriser sa connexion. 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, c'est de n'installer que celles provenant de sources fiables telles que Google Play ou l'App Store (Apple). Des boutiques parallèles, non officielles, en proposent parfois 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 !

QUI A TOUCHÉ À 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. Les logiciels payants qui vous promettent de vous révéler un espionnage sont légion, mais ne vous laissez pas séduire !

> **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#.

Bref, à chaque fois, on fait du cas par cas. Pour cela, dans les réglages de son appareil puis dans «Applications», on sélectionne les autorisations que l'on accorde à chacune, en les limitant aux moments d'ouverture. À noter: certaines restrictions peuvent entraver la bonne marche des applications. Par exemple, interdire la géolocalisation sur une carte routière ou un GPS les >>

EXISTE-T-IL UN TÉLÉPHONE PLUS SÉCURISÉ QU'UN AUTRE ?

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 régulières 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 grosse pomme. Mais attention ! Aucun système n'est parfaitement sûr, et les iPhone peuvent succomber à des attaques et se faire voler leurs informations, notamment par le biais d'applications malveillantes, de réseaux wifi publics ou de techniques d'hameçonnage (phishing).

>> empêche de fonctionner… En revanche, on peut imposer à des applis de se fermer quand elles ne sont plus en service. Il est aussi important de vérifier régulièrement leurs mises à jour: des options peuvent apparaître comme disparaître (accès aux SMS, géolocalisation obligatoire, etc.).

Stockage des données et messageries

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 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.

UN APPAREIL POUR LES VIP

De plus en plus de marques proposent des téléphones portables spécialisés dans la protection de la vie privée. Leurs noms ? Bittium, Blackphone Privy 2.0, Sirin Finney… Leur prix peut atteindre plusieurs milliers d'euros. Ils sont destinés, en priorité, aux personnes ayant des fonctions sensibles (politiciens, journalistes, grands chefs d'entreprise…). Ils proposent chiffrement, contrôle et blocage des cyberattaques, etc.

À ne pas négliger non plus: la sauvegarde régulière de ses données 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 vérifiera également l'utilisation des données qui passent par le téléphone. Pour les propriétaires d'un modèle sous Android, il faut aller dans les options du wifi situé dans les «Réglages» de l'appareil et sélectionner «Utilisation des données». Il suffit ensuite de choisir «Utilisation des données mobiles» (ou des données wifi) pour découvrir les applications les plus consommatrices d'informations personnelles. Les possesseurs d'iPhone, eux, iront dans «Réglages > Données mobiles».

Intéressantes, certaines applications de messagerie sécurisent conversations et messages grâce au chiffrement de bout en bout. Parmi les meilleures, on trouve Signal et Threema (Suisse), Olvid (France), WhatsApp (USA/Meta). 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, on ne clique jamais sur des liens ou des pièces jointes provenant de sources suspectes. Enfin, pour une protection la plus efficiente possible, le destinataire doit se servir de la même appli que l'émetteur. ■

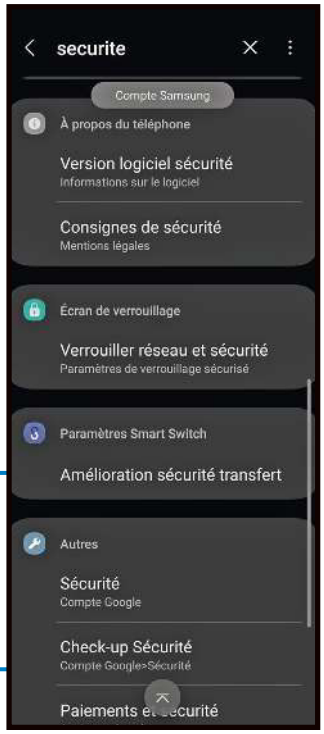
Fiche pratique

CHIFFRER SOUS ANDROID

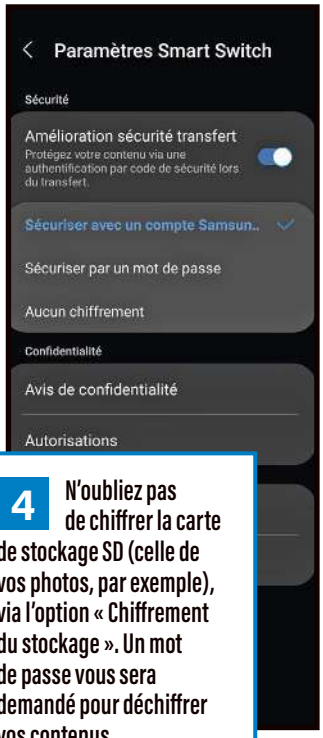
Comme nous l'expliquons dans ce hors-série, chiffrer ses informations personnelles est un moyen quasi imparable de se protéger des regards non autorisés. Si vous possédez un téléphone sous Android, il est possible d'activer le chiffrement pour renforcer votre cybersécurité. Plusieurs méthodes existent, 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, dans 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.

LES 8 PROTECTIONS INDISPENSABLES

La trousse de secours numérique, on n'y pense pas toujours, or elle peut nous sauver ! Voici la liste de base pour assurer sa cybersécurité.

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», en français). Des outils gratuits comme AdwCleaner (Fr.malwarebytes.com) 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 non officielle.

3 LE FIREWALL

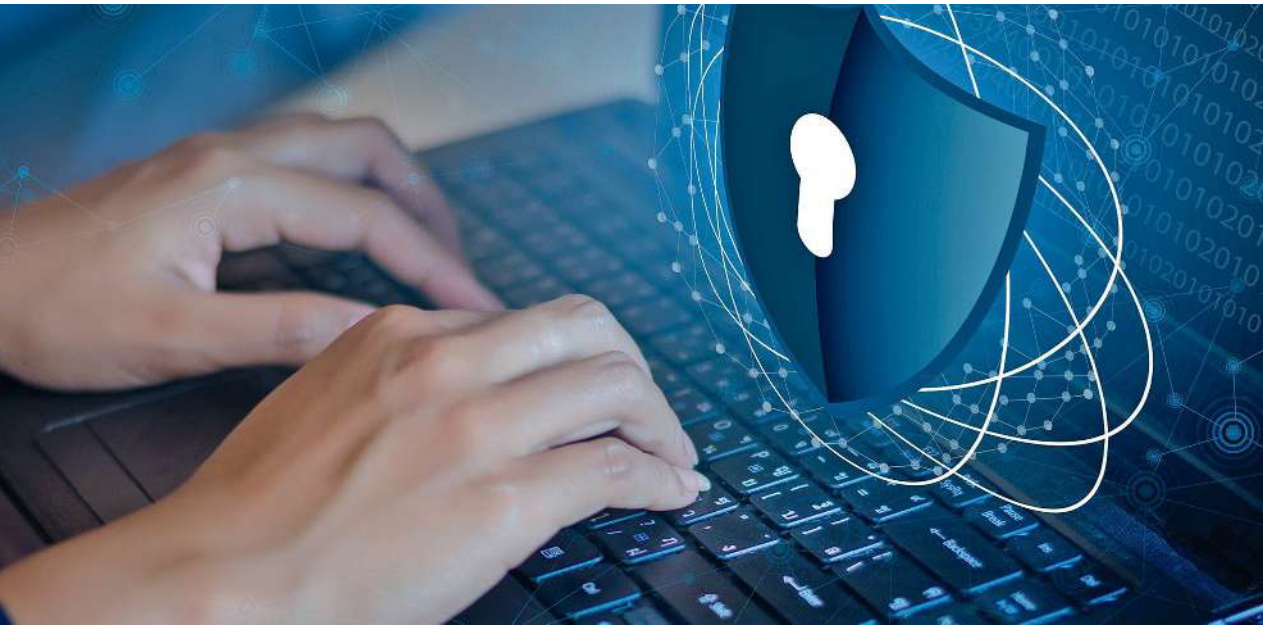
Ce dispositif va contrôler le trafic Internet entrant et sortant de l'ordinateur. Il analyse des «paquets» d'informations et bloque ceux considérés comme dangereux. À partir de la version 10, Windows Defender Firewall, un firewall gratuit est intégré dans le système d'exploitation Windows et activé par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

4 LE VPN

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

5 LA SÉCURITÉ INTÉGRÉE ET LES EXTENSIONS

Les systèmes de navigation classiques comme Firefox, Chrome, Opera ou encore Edge disposent de fonctionnalités de sécurité intégrées telles que la prévention des pop-up, le signalement de sites dangereux ou la protection contre les *trackers* (ces dispositifs 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», comme Adblock Plus ou encore Privacy Badger, l'outil créé par la fondation Electronic Frontier Foundation (Eff.org). Son but: bloquer les sites



SARAYUT_SAN/ADOBE STOCK

web qui tentent d'intercepter des renseignements sur les habitudes de l'internaute. Recourir à une extension de sécurité renforce aussi la sûreté de son navigateur en l'obligeant, par exemple, à refuser tous les sites n'affichant pas le petit cadenas dans la barre d'adresse (signe d'une connexion sécurisée). C'est notamment ce que propose HTTPS Everywhere (Eff.org). 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: le fonctionnement de certains sites légitimes peut en être perturbé.

6 L'AUTHENTIFICATION À DEUX FACTEURS

Indispensable, l'authentification à deux facteurs (2FA) ajoute une «couche» de sécurité supplémentaire 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 sont 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 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 *open source* gratuit BleachBit (Bleachbit.org), 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 avec l'eau du bain.

8 L'ADRESSE JETABLE

Un outil comme SimpleLogin (Simplelogin.io) permet 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. ■

L'OSINT AU SERVICE DU RENSEIGNEMENT

Le renseignement en sources ouvertes, ou Osint, permet à n'importe qui de collecter des quantités incroyables d'informations grâce aux ressources offertes par Internet.

Les termes *Open Source Intelligence*, ou Osint («renseignement en sources ouvertes») désignent l'exploitation de foyers d'information publics ou accessibles à tout un chacun (sites web, forums, journaux, bases de données, conférences…) 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. Jusqu'au XV^e^ siècle, entre la Chine et la Turquie, les caravanes avançant sur la Route de la soie servaient autant au commerce qu'à la collecte d'informations. Durant la Seconde Guerre mondiale, gouvernements, milices et résistants, cherchant à en savoir plus sur leurs adversaires pour mener ou parer des attaques, ont donné à cette pratique un essor particulier, la portant jusque sur le «zinc» des bars et cafés. Quelques années plus tard, l'avènement de la Guerre froide la développera encore, puis Internet et les nouvelles technologies lui confèreront 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. Vous aimeriez bien savoir où le cliché a été pris ? GeoHints.com est capable de vous indiquer la marque du véhicule, mais aussi sa géolocalisation à partir d'une analyse de la bordure du trottoir, des panneaux, des feux de signalisation, des poteaux électriques, etc.

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 le site 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 ce cliché d'un avion furtif B-51

TRAQUER LES PRISONS SECRÈTES DE LA CIA

En 2004, Adrian Shahbaz, étudiant en journalisme à l'université de Columbia, aux États-Unis, a utilisé des techniques d'Osint pour localiser une prison secrète de la CIA en Roumanie, où des individus soupçonnés de terrorisme étaient interrogés. Documents officiels, articles de presse, témoignages d'anciens détenus, images satellites et rapports d'activité de vol ont été passés au crible par l'étudiant pour trouver l'emplacement de la prison. En publiant son enquête, il a contraint la Roumanie à reconnaître l'existence de cette geôle sur son territoire, et les États-Unis ont été critiqués pour leurs méthodes d'interrogatoire. Adrian Shahbaz, devenu un journaliste primé, continue d'investiguer sur les cas de violation des droits de l'homme.

Appliquer l'Osint à soi-même

Tapez votre nom complet sur Google, et voyez ce qui apparaît en haut des résultats de recherche. Il existe de nombreux logiciels (gratuits et payants) permettant de surveiller les réseaux sociaux. Social Mention (Social-searcher.com), par exemple, offre la possibilité de suivre toutes les mentions de votre identité sur Facebook, Twitter, etc. Cet outil démontre, s'il en était encore besoin, l'importance de l'attention à porter aux informations personnelles en ligne…

de l'armée américaine. Le lieu de parking de ce bombardier a été découvert grâce à la position des étoiles, à des 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 d'outils disponibles pour collecter des informations à partir de sources ouvertes. Premiers de tous: les moteurs de recherche. Leur fonctionnalité de base – trouver rapidement des données depuis des mots-clés spécifiques – en fait de précieux alliés. Viennent ensuite les réseaux sociaux. De fait, Facebook, Twitter, LinkedIn ou Instagram sont de vraies pipelettes! Ils permettent de trouver des éléments sur les activités de leurs abonnés, leurs centres d'intérêt, leur emploi du temps, leurs vacances, etc. Enfin, les solutions de cartographie telles Google Maps ou Bing Maps fournissent des renseignements sur les lieux, les bâtiments, les routes et les itinéraires. Bref, autant d'instruments de recherche que les espions de la Guerre froide auraient pu nous envier… ■

ENQUÊTE SUR LES RÉSEAUX SOCIAUX

Le groupe Bellingcat, un collectif d'enquêteurs en ligne, a utilisé des techniques d'Osint pour aider la police à résoudre le mystère du crash du vol MH17 de Malaysia Airlines, abattu au-dessus de l'Ukraine en 2014. Les journalistes ont analysé des images satellites, des vidéos de témoins, des photos publiées sur les réseaux sociaux et des enregistrements audio pour reconstituer la trajectoire de l'avion et celle du missile qui l'a touché. En utilisant des documents gouvernementaux et des registres de transport, ils ont identifié l'unité du renseignement militaire russe responsable du tir fatal. L'enquête de Bellingcat a contribué à établir la responsabilité de la Russie dans cette affaire, illustrant au passage l'importance de l'Osint dans la recherche de la vérité.

MUSTAFAHACALAKI/ISTOCK

SOMMAIRE

Se faire aider

Si vous constatez une fuite de vos données personnelles, la priorité est de vous protéger et de vous faire aider, afin que ce piratage numérique ne se transforme pas en enfer. Se sentir embarrassé d'avoir été trompé est normal, mais rappelez-vous toujours qu'il n'y a pas de honte à être la victime d'une fraude, et que nul n'est épargné. Les malfaiteurs sont de plus en plus habiles, leurs actions de plus en plus sophistiquées, ce qui rend la menace très difficile à détecter et à contrer. Prévenir les autorités, c'est vous sauver et sauver les autres ! Dans ce chapitre, nous vous présentons les sites de premiers secours à contacter en cas de fraude numérique, ainsi que les conseils avisés du Gal Marc Boget, patron du Commandement de la gendarmerie dans le cyberespace (ComCyberGend), et de Jérôme Notin, directeur général de la plateforme nationale Cybermalveillance.

J. SAGET/AFP

À LA RECHERCHE DES DONNÉES PERDUES

Nous avons tous connu ce moment difficile où nous avons accidentellement supprimé des fichiers importants de notre ordinateur, de notre téléphone portable ou de notre clé USB. Pas de panique ! Des solutions existent.

Perdre des données est aussi simple qu'un clic de souris… et les causes les plus fréquentes sont accidentelles. La première – qui n'est pas définitive –, tient dans la suppression malencontreuse d'un fichier important, qui se retrouve alors à la poubelle. Heureusement, 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 (également rattrapable), le déplacement intempestif: un «glissé» malheureux, et voilà votre fichier disparu dans les méandres de l'ordinateur. Ici aussi, pas de panique, la commande proposée plus haut viendra à votre secours. Mais d'autres situations s'avèrent plus dramatiques. Citons le formatage accidentel. Vous êtes en train de formater votre support numérique et, tout à coup, vous vous rendez compte que vous avez oublié de sauvegarder des données importantes ! Et c'est trop tard. Il y a aussi la panne matérielle et l'écrasement de fichiers. Enfin, ces derniers peuvent être pris en otages par un code malveillant (rançongiciel, cryptolocker) ou subir l'attaque d'un virus qui les détruit ou les endommage.

Sauver ce qui peut l'être sur un ordinateur

Il existe plusieurs logiciels gratuits capables d'aider à retrouver des données effacées. Mais attention, si vous vous rendez compte de l'erreur fatale, stoppez toute utilisation 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 encore 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. L'analyse terminée, l'outil vous indique ce qui peut être sauvé. Attention, selon la taille et le type de document (texte, image, vidéo), la récupération risque d'être partielle.

Récupérer des fichiers effacés d'un smartphone

La complexité des téléphones portables de nouvelle génération, véritables «ordiphones», laisse peu de chances de retrouver un fichier, une photo ou une vidéo effacée… Pour un appareil sous Android, des outils comme EaseUS MobiSaver, Dr. Fone, DiskDigger ou Recuva annoncent pouvoir vous aider. Il est cependant important de noter que récupérer des données n'est pas garanti. Par sa nature, le smartphone enregistre en permanence des informations; la récupération peut donc ne pas être possible en raison d'une surécriture… Sur un téléphone, la meilleure méthode pour ne pas perdre ses données, c'est de les sauvegarder très régulièrement.

Reprendre la main sur les réseaux

Vous pouvez récupérer l'ensemble des éléments que vous avez diffusés sur un réseau social depuis votre inscription. Chaque plateforme possède ses propres fonctionnalités de récupération d'archives et de données (sauf Snapchat). Nous vous indiquons ici celles à connaître sur deux des plus populaires, Facebook et Instagram.

> **Facebook** Connectez-vous à votre compte. Tapez sur la flèche en haut à droite de l'écran

En cas d'effacement malencontreux, des logiciels gratuits peuvent scanner le support de stockage de l'ordinateur et vous indiquer ce qui est récupérable.

et allez dans « Paramètres et confidentialité ». Dans la section « Vos informations Facebook », cliquez sur « Télécharger vos informations ». Sélectionnez les données que vous souhaitez récupérer (par exemple, vos publications, photos, vidéos, messages, etc.). Allez sur « Créer un fichier » et attendez que Facebook génère votre archive. Dès que cela est terminé, Facebook vous envoie un lien pour la télécharger.

> **Instagram** Connectez-vous à votre compte. Rendez-vous sur votre profil et cliquez sur les trois lignes en haut à droite de l'écran. Choisissez alors « Paramètres », puis « Sécurité ». Cliquez sur « Télécharger les données ». Sélectionnez celles que vous voulez récupérer (par exemple, vos photos, vos vidéos, vos commentaires, vos messages, etc.). Cliquez sur « Demander un téléchargement », puis attendez qu'Instagram génère votre archive. Une fois qu'elle est réalisée, vous recevrez un lien pour l'importer. ■

LE TOP 3 DE LA RÉCUPÉRATION

> **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 récupérés. Mais attention, ne sauvegardez plus aucun fichier sur le support avant de lancer une procédure de récupération.
Cgsecurity.org/wiki/PhotoRec_FR

Interview

MARC BOGET Général de division, commandant de la gendarmerie dans le cyberespace

« LE PLUS GRAND RISQUE, C'EST L'IGNORANCE »

Son unité ComCyberGend fédère les différents services spécialisés dans la lutte contre les menaces en ligne. Rencontre avec le général de division Marc Boget.

Quel est le rôle de l'unité que vous commandez ?

Marc Boget Le Commandement de la gendarmerie dans le cyberespace (également appelé ComCyberGend) existe depuis février 2021. Rattachée à la direction générale de la gendarmerie nationale, cette unité est née de la volonté du général Christian Rodriguez, convaincu de l'importance du sujet. Notre mission ? Définir et mettre en œuvre la lutte contre la cyberdélinquance. Elle s'articule autour de quatre axes: 1. la prévention et la proximité avec la population, notamment grâce au site Ma Sécurité et à de nombreuses campagnes de sensibilisation; 2. les enquêtes et les interventions menées par la Division des opérations du Centre de lutte contre les criminalités numériques (DO-C3N); 3. l'expertise technique pour, entre autres, développer des outils d'investigation; et enfin 4. les partenariats avec les acteurs de l'écosystème cyber. La formation continue des 9 000 cybergendarmes présents partout sur le territoire fait également partie des missions du ComCyberGend. Ces officiers et sous-officiers ont des profils très variés; ils ajoutent à leur expérience du terrain des compétences d'enquêteurs, d'ingénieurs, de spécialistes de la cryptographie ou encore des algorithmes.

Partout en France, les cybergendarmes distillent des conseils personnalisés

Pouvez-vous nous préciser les domaines d'intervention de ces cybergendarmes ?

M. B. Nous comptons de nombreux spécialistes dans nos rangs. Parmi eux, des enquêteurs dans le numérique (NTech), d'autres en charge de la pédocriminalité, mais aussi des experts œuvrant dans des secteurs variés. Quelques exemples ? Les messageries chiffrées, les crypto-actifs (Fintech), la recherche en sources ouvertes [Open Source Intelligence, ou Osint] et en données massives, la récupération et l'analyse de datas, ou encore la prospective et l'anticipation par les technologies numériques émergentes. Ces divers champs d'intervention exigent une solide expérience, qu'il faut coupler avec des aptitudes pédagogiques afin de dispenser des conseils adaptés aux publics visés. ComCyberGend a également en charge, pour la gendarmerie nationale, la plateforme d'assistance aux victimes de violences sexuelles et sexistes.

L'éducation est-elle la meilleure protection contre les risques en ligne ?

M. B. Oui, et la gendarmerie y prend toute sa part. Partout en France, et auprès de tous les publics, les militaires du réseau CyberGend distillent des conseils personnalisés. Aux plus jeunes, par exemple,

M.A. SAILLET

nous inculquons les bases de l'hygiène numérique avec le «Permis internet» et le dispositif Protect. C'est une priorité pour la gendarmerie, qui s'est investie depuis longtemps au profit des enfants et des séniors, car une de nos missions prioritaires est de protéger les plus vulnérables.

QC La formation à la cybersécurité devrait commencer dès le plus jeune âge ?

M. B. Tout à fait ! Les dernières générations sont nées avec l'outil numérique. Il faut leur apprendre au plus tôt les bons réflexes. Ici, les parents ont un rôle clé à jouer, et il existe pour les aider de nombreuses publications gratuites et ludiques à destination des enfants, sur E-enfance.org ou Cybermalveillance.gouv.fr, par exemple. En plus de cela, les parents doivent rassurer les jeunes usagers et les inviter à signaler immédiatement tout contenu qui les interroge. Le plus grand risque dans le domaine de la cybercriminalité, c'est l'ignorance. Le maillon faible de la sécurité, c'est l'humain. Moins il connaîtra les bonnes pratiques et plus il ouvrira la boîte de Pandore, avec le risque qu'à la fin il ne lui reste plus que l'espoir, comme dans cette histoire…

QC Les pirates ne sont pas invincibles. Vous les traquez sans relâche même s'ils sont à l'étranger, n'est-ce pas ?

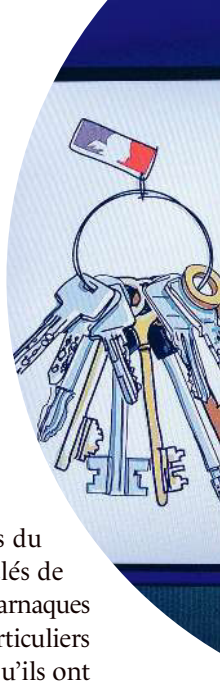
M. B. En effet. En matière de rançongiciels, par exemple, certaines investigations sont menées depuis plus de deux ans. Le cyberespace ne connaît pas de frontières et nous nous appuyons sur la coopération policière internationale pour rassembler toutes les preuves dont nous avons besoin afin d'identifier les criminels. C'est ainsi qu'au début de l'année nous avons pu interpeller plusieurs individus à l'étranger, et saisir ou geler près de 20 millions d'euros d'argent liquide ou de crypto-actifs. Contrairement à un cambriolage ou une agression physique, pour lesquels les investigations se déroulent essentiellement en France, les infractions commises dans le cyberespace impliquent quasi systématiquement la recherche de la coopération policière à l'international.

QC Quels conseils donneriez-vous à nos lecteurs en matière de sécurité ?

M. B. Il faut protéger son ordinateur avec un mot de passe fort, un antivirus, un pare-feu et des mises à jour de sécurité régulières. Pour préserver son intimité, il convient de rester discret, et de toujours être prudent lorsque l'on reçoit des courriels et des pièces jointes d'inconnus (par défaut, on ne les ouvre pas). Mieux vaut s'abstenir de naviguer sur des sites suspects. En cas de message alarmant, on ne se précipite pas, car les fraudeurs misent toujours sur la panique et le sentiment d'urgence. Avant de partir en vacances, on ne publie pas ses dates et lieu de villégiature. Enfin, il est utile de signaler à la gendarmerie dont on dépend ses jours de départ et de retour de voyage. Dans le cadre de l'opération «Tranquillité vacances», des militaires exerceront une surveillance renforcée du domicile. ■

LES SITES DE PREMIERS SECOURS

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



CYBERMALVEILLANCE.GOUV.FR

Cette plateforme gouvernementale propose une assistance gratuite aux internautes. Elle leur donne la possibilité de déclarer les actes de cybercriminalité dont ils ont été victimes, mais aussi d'obtenir des conseils et des solutions pour y faire face. Une mise en relation avec des entreprises privées (payante) est permise.

LA BRIGADE NUMÉRIQUE DE LA GENDARMERIE NATIONALE

Créée en 2018, cette unité propose de discuter en ligne avec un gendarme, via un service de tchat disponible 7 jours sur 7 et 24 heures sur 24. Vous pouvez lui poser des questions, lui signaler un délit ou une fraude en ligne, lui demander une assistance en cas de cyberharcèlement ou d'usurpation d'identité, etc. L'adresse à enregistrer: **Gendarmerie.interieur.gouv.fr/contact/discuter-avec-un-gendarme.**

RÉAGIR EN CAS D'ESPIONNAGE

Dirigeant d'une PME/PMI, vous êtes détenteur d'un savoir-faire unique. Derrière un acte de malveillance informatique à l'encontre de votre société, peut se cacher un espion. Au moindre doute, alertez la Direction générale de la sécurité intérieure (DGSI). Parmi ses missions, la criminalité organisée et les atteintes à la sécurité nationale. Pour la contacter : **Dgsi.interieur.gouv.fr/contacter-nos-services.**

INFO ESCROQUERIES

La plateforme Info Escroqueries du ministère de l'Intérieur fournit des clés de compréhension des différentes formes d'arnaques en ligne. Elle permet également 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 gratuit), du lundi au vendredi, de 9 h à 18 h 30.

MA SÉCURITÉ

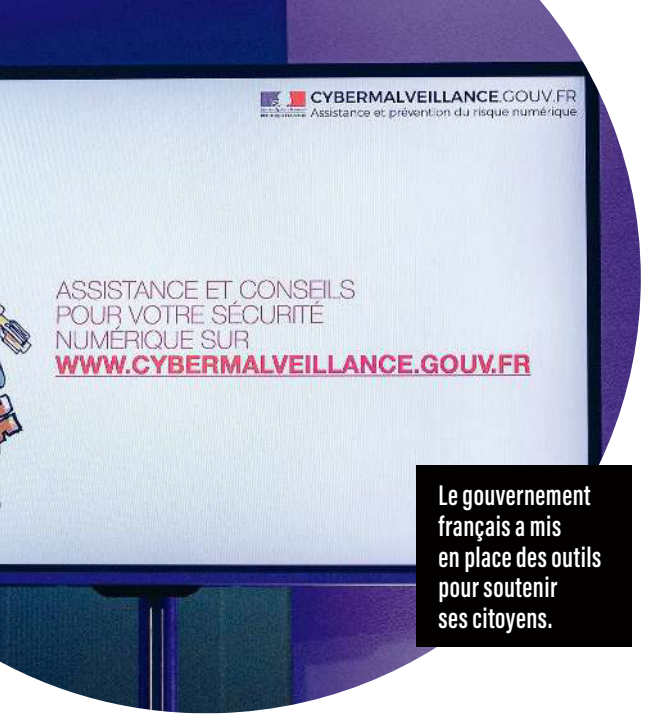
Auparavant nommé Moncommissariat.fr, **Masecurite.interieur.gouv.fr** délivre des informations utiles (annuaire des commissariats et gendarmeries, fiches pratiques sur les arnaques, etc.). Policiers et gendarmes y accompagnent tout un chacun dans ses démarches. Sur la page d'accueil, un onglet permet d'accéder au service de traitement harmonisé des enquêtes et signalements pour les e-escroqueries (Thésée) et de déposer plainte.

PHAROS

La Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) a été créée par le ministère de l'Intérieur. Dédiée à la lutte contre les propos ou des comportements illégaux sur Internet, elle propose également une assistance en cas de délit informatique. L'adresse à enregistrer: **Internet-signalement.gouv.fr.**

L'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (Anssi) fournit des conseils et une assistance aux particuliers comme aux entreprises. Elle offre également des formations pour sensibiliser aux bonnes pratiques, ainsi que



Le gouvernement français a mis en place des outils pour soutenir ses citoyens.

des audits de sécurité pour évaluer les vulnérabilités des systèmes informatiques. L'adresse à enregistrer: **Ssi.gouv.fr.**

E-ENFANCE

Reconnue d'utilité publique, l'association e-Enfance assure une mission de protection des plus jeunes sur Internet et d'éducation à la citoyenneté numérique. Sur son site, les parents peuvent, entre autres, trouver des conseils pour protéger leur progéniture des pièges du Web. Surtout, elle offre une assistance aux enfants et adolescents victimes de cyberharcèlement, grâce au numéro court et à l'application 30 18. L'adresse à enregistrer: **E-enfance.org.**

POINT DE CONTACT

Cette plateforme a été lancée par l'Union européenne pour que les internautes puissent 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.**

PRÉ-PLAINTE EN LIGNE

Ce service ministériel permet d'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: **Pre-plainte-en-ligne.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. Son site les informe sur leurs droits, et leur fait des recommandations pour se prémunir des atteintes sur Internet. L'adresse à enregistrer: **Cnil.fr.**

SIGNAL SPAM

Cette plateforme permet de 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.** ■

CYBERATTAQUE
LES 7 BONS RÉFLEXES

Vous venez d'être victime d'une attaque numérique ? Voici les actions à mener.

1. **Alertez immédiatement votre banque** en cas de fuite de vos données bancaires (à la suite d'un hameçonnage, etc.).
2. **Gardez toutes les preuves** (captures d'écran, tchat, courrier électronique, 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.

IC. MORIN/IP3 PRESS-MAXPPP

ANTIVIRUS
SÉCURISEZ VOS APPAREILS

Les outils de protection sont de diverses natures, comme leurs options. Solution intégrée ou dédiée ? Version gratuite ou payante ? Nos conseils.

Des millions de logiciels malveillants apparaissent chaque année: espions visant à récupérer les informations de votre ordinateur, chevaux de Troie pour en prendre le contrôle, rançongiciels pour bloquer votre machine jusqu'au paiement d'une rançon (si cela vous arrive, ne payez pas !), tentatives de phishing pour récolter des données personnelles… Les pirates ne manquent pas d'imagination. Sur PC, un antivirus est une sage précaution.

Nous avons testé 13 solutions pour vérifier leur efficacité ainsi que leur facilité d'utilisation, et pour comprendre les différences entre les logiciels gratuits et payants. Le premier constat est plutôt rassurant: leurs performances sont suffisantes pour la plupart des usages. Le deuxième bilan l'est un peu moins, puisqu'aucune solution n'est parfaitement infaillible… Par erreur, les antivirus arrêtent parfois des fichiers anodins, alors qu'ils en laissent passer d'autres plus virulents. Pas de quoi, cependant, remettre en cause leur utilité.

Ressources consommées

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. Car comme tout logiciel, il consomme les ressources de votre machine (espace sur le disque dur, mémoire vive) et sollicite le processeur pour l'exécution de ses tâches. Ainsi, le meilleur du test, G Data Internet Security (dont vous pouvez suivre l'installation en p. 102) occupe 3 gigaoctets (Go) sur votre disque dur: c'est beaucoup, surtout si ce dernier est limité. Vous constaterez, dans notre tableau de résultats, que les solutions payantes ne sont pas plus efficaces que les gratuites. Dès lors, pourquoi payer ? En fait, cela permet d'accéder à des services annexes: VPN (réseau privé virtuel) pour protéger votre connexion à Internet, pare-feu propriétaire, gestionnaire de mots de passe, contrôle parental, sauvegarde en ligne, etc. Mais ces fonctions donnent surtout aux éditeurs de logiciels l'opportunité de se distinguer les uns des autres, et de convertir les utilisateurs d'outils gratuits aux versions payantes… Notre suivi régulier révèle par ailleurs que ces fonctionnalités vont et viennent au gré des mises à jour: il n'est pas impossible qu'elles disparaissent sans préavis. Dès lors, pour profiter d'un service de stockage dans le cloud ou d'un gestionnaire de mots de passe, mieux vaut opter pour une offre dédiée (lire aussi p. 37 et 62). ■

MONSTER ZTUDIO/ADOBE STOCK

Test

13 SOLUTIONS GRATUITES OU PAYANTES

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

		Facilité d'emploi											
		PROTECTION	INSTALLATION/ DÉSINSTALLATION	IMPACT PERFORMANCES DE L'ORDINATEUR	UTILISATION	APPRÉCIATION GLOBALE		PRIX (1)	PARE-FEU PROPRIÉTAIRE	GESTIONNAIRE DE MOTS DE PASSE	SAUVEGARDE EN LIGNE (CLOUD FABRICANT)	VPN	CONTRÔLE PARENTAL
						Note sur 20		€					
1	**G DATA** INTERNET SECURITY	★★★	★★	★★★	★★★	**17,3**	★★★	56	●	-	-	-	●
2	**AVAST** ONE INDIVIDUEL	★★★	★★★	★★★	★★★	**17,2**	★★★	90 (2)	●	-	-	●	-
3	**BITDEFENDER** INTERNET SECURITY	★★★	★★	★★	★★★	**17,1**	★★★	65	●	●	-	●	●
4	**BITDEFENDER** ANTIVIRUS FREE	★★★	★★★	★★★	★★	**17,1**	★★★	Gratuit	-	-	-	-	-
5	**NORTON** 360 DELUXE	★★★	★★	★★★	★★★	**17**	★★★	95 (2)	●	●	●	●	●
6	**AVAST** ONE ESSENTIEL	★★★	★★★	★★	★★	**16,7**	★★★	Gratuit	●	-	-	●	-
7	**MCAFEE** TOTAL PROTECTION	★★★	★★	★★★	★★	**16,7**	★★★	110 (2)	●	●	-	●	-
8	**F-SECURE** TOTAL	★★★	★★★	★★★	★★	**16,6**	★★★	100	-	●	-	●	●
9	**ESET** INTERNET SECURITY	★★	★★★	★★★	★★★	**16**	★★	65	●	-	-	-	●
10	**AVIRA** FREE SECURITY	★★	★★	★★★	★★	**15,5**	★★	Gratuit	-	●	-	●	-
11	**AVIRA** ANTIVIRUS PRO	★★	★★	★★★	★★	**15,4**	★★	45	-	●	-	●	-
12	**TREND MICRO** INTERNET SECURITY	★★	★★	★★★	★★	**14,8**	★★	60	-	-	-	-	●
13	**MICROSOFT** DEFENDER (3)	★★	★★★	★★★	★★	**14,3**	★★	Gratuit	-	-	-	-	-

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

NOTRE MÉTHODE

Nos tests évaluent la capacité à protéger votre ordinateur. Nous visitons 100 sites hébergeant des éléments malveillants, connectons une clé USB infectée et stockons 10 000 fichiers problématiques (troyens, vers, virus, espions). Par ailleurs, nous vérifions la facilité d'utilisation du logiciel (son installation et sa désinstallation, l'espace occupé, la rapidité d'exécution, etc.).

Le meilleur

G DATA TRUST IN GERMAN SICHERHEIT

G Data INTERNET SECURITY
56 € **17,3/20 | ★★★**

Ce logiciel simple à utiliser procure un très bon niveau de protection. Le blocage des sites d'hameçonnage, qui fonctionne via une extension à installer dans le navigateur, se révèle assez efficace, avec le blocage de 87 % d'entre eux. En outre, G Data ne ralentit pas l'ordinateur. Précision : le renouvellement de la licence est automatique ; si vous renoncez sur le moment pour vous réabonner plus tard, le prix passera à 120 €.

L'alternative

Microsoft

Microsoft DEFENDER
Gratuit **14,3/20 | ★★**

Votre ordinateur, s'il fonctionne sous Windows 10 ou 11, intègre Windows Defender : vous n'avez rien à installer, et c'est gratuit ! Sa position de dernier du classement ne doit pas vous refroidir, elle ne tient qu'à l'absence d'antiphishing dont, désormais, tous les navigateurs sont dotés d'office… Et la solution protège efficacement des menaces ; elle peut donc tout à fait convenir à qui souhaite aller au plus simple.

Pas-à-pas

INSTALLER ET CONFIGURER G DATA

- **Objectif :** profiter du meilleur outil de protection payant.
- **Niveau de difficulté :** facile.
- **Temps nécessaire :** 5 à 10 minutes.

La bonne solution selon les besoins de chacun

Les versions 10 et 11 du système d'exploitation Windows intègrent l'antivirus Microsoft Defender et le pare-feu de Windows, deux protections essentielles. Par contre, le filtrage des pages internet malveillantes (antiphishing) est laissé aux soins du navigateur que vous utilisez (Edge, Chrome, Firefox…). Sur le marché, des antivirus payants, comme G Data, offrent une protection supérieure à celle de Windows Defender – surtout sur l'anti-hameçonnage – et éventuellement des fonctionnalités supplémentaires (contrôle parental, antispam…). Cependant, si ces options ne vous sont pas nécessaires, préférez la version gratuite de Bitdefender, tout aussi robuste.

Faire barrage aux spams

Le filtrage des e-mails indésirables par un antivirus ne fonctionne que lorsque leur consultation a lieu via un logiciel dédié comme Outlook, Thunderbird ou Windows Mail. Mais si vous lisez vos messages depuis une page web comme Gmail, La Poste ou Yahoo!, l'antispam ne peut pas agir, et sa mise en place est sans objet.

Un antivirus étant gourmand d'espace, n'installez que les éléments que vous utiliserez

G Data Internet Security, une solution personnalisable

Contrairement à plusieurs de ses concurrents, G Data autorise un essai pendant 30 jours sans entrer son numéro de carte bancaire: profitez-en ! Et il est aussi possible de personnaliser le fonctionnement de ce logiciel. Comme il est plutôt gourmand en espace disque, n'installez pas les éléments que vous n'utiliserez pas (images 1 et 2); par exemple, si votre foyer ne compte pas d'enfant, le contrôle parental est superflu. Par ailleurs, G Data peut détecter la présence des navigateurs web les plus courants (Chrome, Edge et Firefox) et vous proposer des extensions (image 3) de détection et de blocage de sites malveillants. Attention: il ouvrira chaque navigateur aux pages correspondantes, mais vous devrez procéder à l'installation des extensions vous-même (image 4).

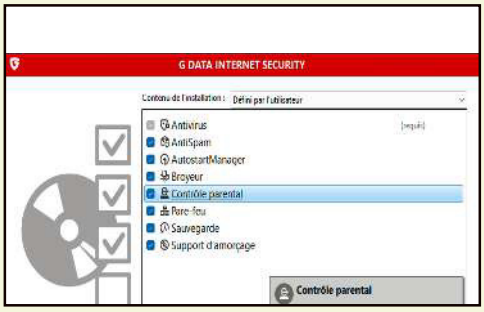
Bitdefender Antivirus Free, un outil discret

Ce logiciel est un très bon produit, mais il est bien difficile à trouver sur le site internet dédié ! Vous y parviendrez en tapant son nom complet dans votre moteur de recherche. Précisez bien *free* («gratuit»), sinon vous risquez de tomber sur les pages correspondant aux versions payantes de cet antivirus ou sur celles de ses concurrents. Son interface est explicite, et comme il comporte peu de fonctions annexes, il n'y a pas de réglage à faire – sauf désactiver les notifications d'offres spéciales ou de recommandations si elles s'avèrent envahissantes. ■

Par **Patrick Gérard** (HC Lab)

Les étapes essentielles

1 L'antivirus G Data, premier de notre classement, permet une installation personnalisée, élément par élément, afin d'adapter le logiciel à vos besoins.



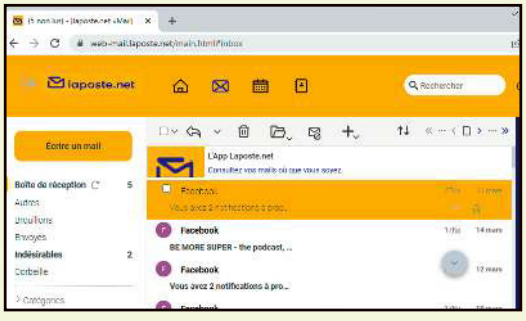
2 Pour choisir les éléments à installer, il faut sélectionner « Défini par l'utilisateur » (en haut à droite de la fenêtre).

3 Une fois vos navigateurs web détectés, G Data vous proposera d'ajouter des extensions de détection et de blocage de sites malveillants.

4 C'est à vous de mettre manuellement en place de ces extensions, en œuvrant depuis leur page d'installation sur Internet.

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.



Si vous consultez vos e-mails via une page internet (ici, Laposte.net), l'antispam de l'antivirus ne peut pas fonctionner, c'est donc inutile de l'installer.

L'ANTIVIRUS EN LIGNE, UNE BONNE SOLUTION ?

Souvent gratuits, les sites d'antivirus ne nécessitent pas d'installation sur votre ordinateur. Ils sont faciles à utiliser et efficaces, mais ils ont aussi 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 mettent en œuvre une combinaison de techniques pour repérer les attaques. Les méthodes 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 virus 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 détecter les menaces du type adresses web ou fichiers piégés. Ils permettent de passer au peigne fin des éléments ou des liens suspects. VirusTotal, par exemple, propose un service gratuit d'analyse qui exploite plus de 60 antivirus. L'internaute soumet un lien ou télécharge un fichier suspect directement sur le site de VirusTotal, et le rapport d'analyse est généré en quelques dizaines de secondes (selon la taille du fichier).
Il faut toutefois être conscient qu'envoyer ainsi des documents – Word, Excel, ou autre – potentiellement sensibles, c'est courir le risque de compromettre leur confidentialité (lire aussi p. 108). Enfin, il est à noter que certains pirates testent leurs créations sur VirusTotal avant de

310 000 NOUVEAUX FICHIERS MALVEILLANTS PAR JOUR !

Virus, vers, chevaux de Troie, logiciels espions ou encore rançongiciels : les fichiers vérolés pullulent sur la Toile. Selon l'éditeur d'antivirus français AxBx, en février 2023, un internaute avait, par rapport à 2021, six fois plus de risque d'être exposé à un *malware* de type voleur de mot de passe et quatre fois plus de risque de rencontrer un *ransomware*. Les malfaiteurs se servent de différents modes de diffusion pour infecter les systèmes informatiques. Le plus classique reste le phishing, soit l'expédition d'e-mails contenant des liens renvoyant vers des sites usurpant ceux d'organismes connus (banques, opérateurs de téléphonie, Assurance maladie…). Les codes malveillants se répandent aussi par le biais de téléchargements de logiciels piratés ou de faux programmes. Autre cas, les sites web malintentionnés. Ils sont conçus pour lancer l'installation d'un logiciel piégé ou mener une cyberattaque dès qu'un visiteur s'y connecte. Enfin, prudence avec les périphériques de stockage inconnus : il est assez simple de placer un fichier infecté dans un disque dur externe ou de modifier une clé USB afin d'exfiltrer vos données…

Un logiciel mis à jour en continu se révèle souvent plus efficace.

PIXEL-SHOT/ADOBE STOCK

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

Des atouts de taille

Face aux antivirus traditionnels, parfois lourds, qu'il faut installer sur un ordinateur, ceux en ligne présentent divers avantages. Tout d'abord, ils sont plus faciles à utiliser, puisqu'ils ne nécessitent ni installation ni mise à jour manuelle. De plus, ils sont généralement gratuits, ce qui les rend accessibles à tous. Enfin, ces outils se révèlent souvent plus efficaces, car ils sont actualisés en permanence pour lutter contre les nouvelles menaces dès leur apparition. C'est un véritable atout par rapport aux antivirus traditionnels, car de nombreux internautes pensent qu'une fois qu'ils en ont installé un sur leur ordinateur, ils sont protégés et n'ont plus rien à faire… Or, s'ils oublient de réaliser les indispensables mises à jour des signatures de virus et autres codes malveillants, leur logiciel de sécurité ne servira vite plus à grand-chose ! >>

QUELQUES VIRUS CÉLÈBRES

> **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 informatiques 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 USA 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

JÉRÔME NOTIN Directeur général
de Cybermalveillance.gouv.fr

« LES FRANÇAIS DOIVENT SE FORMER FACE AUX MENACES »

Depuis 2017, une plateforme gouvernementale aide les particuliers, les entreprises et les collectivités à prévenir et à gérer les attaques informatiques. Nous avons rencontré Jérôme Notin, son directeur général.

Pouvez-vous nous expliquer ce qu'est Cybermalveillance.gouv.fr ?

Jérôme Notin Cette plateforme est pilotée par le Groupement d'intérêt public Action contre la Cybermalveillance (GIP Acyma) – sachant qu'un GIP est une structure juridique avec des acteurs publics et privés qui ont mis leurs moyens en commun pour mener une mission d'intérêt général. La nôtre comporte trois volets: l'assistance, la prévention et l'observation de la menace. Ainsi, nous apportons un soutien aux victimes – qu'il s'agisse de particuliers, d'entreprises, de collectivités… –, mais nous nous attachons également à informer les Français sur les menaces numériques et à leur apprendre à s'en protéger.

Concrètement, comment cette plateforme aide-t-elle les internautes ?

J. N. D'abord, en leur fournissant de l'information. Nous produisons beaucoup de documents pour promouvoir les bonnes pratiques, et notre site donne des conseils afin d'améliorer la sécurité numérique, de détecter les menaces et de réagir en cas d'attaque. Sur Cybermalveillance.gouv.fr, l'usager suit un parcours d'assistance via des questions comme «Quel type de cyberattaque ?», «Combien de machines impactées ?» ou encore «Dans quelle région ?». Les réponses apportées vont nous permettre de fournir des conseils personnalisés. Si le problème est technique et nécessite une intervention – une machine bloquée, notamment –, il est possible de la demander à un prestataire de proximité.

65 % des mises en relation avec des prestataires ont lieu en moins d'une heure

Comment se passe cette mise en relation avec un professionnel ?

J. N. Vous venez, par exemple, de vous faire piéger par un rançongiciel, et votre ordinateur est bloqué. Allez sur Cybermalveillance.gouv.fr et répondez aux questions pour décrire votre situation, puis tapez votre code postal. Vous recevrez une liste d'au moins trois entreprises capables de vous dépanner; ne reste qu'à choisir votre préférée. Aujourd'hui, 65 % des mises en relation aboutissent en moins d'une heure, même le week-end.

De quelle façon un prestataire peut-il intégrer votre plateforme et proposer ses services ?

J. N. PME et grandes entreprises de la cybersécurité remplissent un questionnaire sur notre portail. Nous décidons ensuite si elles répondent à nos exigences et sont en mesure d'apporter un soutien technique aux victimes de cyberattaques (25 % des

P. MOREL

demandes sont refusées). Notre site répertorie actuellement 1 200 professionnels dans toute la France, y compris en Outre-mer. Parmi eux, 200 ont obtenu notre label ExpertCyber.

QC La prévention est-elle LA solution face aux attaques en ligne ?

J. N. Oui, sans aucun doute. Notre mission est de renforcer la résilience de la société française face aux cybermenaces, en favorisant la diffusion de bonnes pratiques. C'est pourquoi nous passons beaucoup de temps et dépensons beaucoup d'énergie à produire des contenus. Sans éducation, les internautes continueront de tomber dans des pièges de plus en plus sophistiqués… Ils n'ont pas conscience des risques et cela doit changer, pour le bien de tous. En 2022, nous avons interrogé des responsables de collectivités: 65 % d'entre eux ne se sentaient pas concernés par la menace numérique ! « Pourquoi nous attaquerait-on ? », déclaraient-ils souvent. Or, il faut savoir que les deux piliers de la cybersécurité sont la technique et l'humain. Il importe donc de se mettre dans le même état d'esprit ici que lorsqu'on achète une voiture ou que l'on protège son domicile. Aujourd'hui, quand on construit un bâtiment, plus personne n'hésite à y mettre des extincteurs, des sorties de secours, etc. De même, au moment de se doter d'un système d'information (ordinateur, serveur, boîte électronique, etc.), les entreprises, les collectivités locales et les particuliers doivent s'interroger et voir comment ils le protègent et s'assurent que tout ira bien.

QC N'importe quel citoyen peut-il contribuer à la cybersécurité ?

J. N. Oui, en prenant connaissance de nos contenus d'information – que ce soient les vidéos, les affiches ou les livrets – et en les diffusant autour de lui. Ils sont faits pour cela ! Les personnes un peu plus éduquées à la cybersécurité doivent être des ambassadeurs auprès de leurs proches, de leur famille, de leurs voisins, de leurs collègues… Bref, nous sommes tous des relais utiles.

QC Quels sont vos propres réflexes pour protéger vos données personnelles sur Internet ?

J. N. Je fais très fréquemment des sauvegardes que je déconnecte de ma machine et que je range dans un endroit sécurisé. Je m'assure que mon antivirus est à jour. Je publie très peu sur les réseaux sociaux et mes diffusions sont contrôlées – je ne dis pas quand je pars en vacances, par exemple, car cela peut m'éviter de me faire cambrioler ! Quand je rentre de congés, je m'assure que mes machines (ordinateur, téléphone) sont mises à jour. Je n'hésite pas à changer certains mots de passe dans mon portable. Ces sésames doivent être souvent modifiés ! ■

Les outils en ligne n'analysent le contenu de votre machine que lorsque vous les lancez, la protection est donc ponctuelle.

>> Mais également des désavantages

Les antivirus en ligne présentent cependant des inconvénients. Tout d'abord, ils nécessitent une connexion à Internet à haut débit pour fonctionner, ce qui constitue donc un frein réel si l'on n'en dispose pas. Surtout, ils peuvent poser des problèmes de confidentialité (lire plus haut), car ils ont besoin d'obtenir l'accès à vos fichiers pour les analyser. Un exemple de mésaventure que cela peut entraîner ? En 2017, un consultant travaillant pour la NSA, le service secret américain, a perdu le contrôle de fichiers ultraconfidentiels appartenant à cette agence de sécurité nationale après que son logiciel a détecté des codes malveillants. Par la suite, le consultant 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 peuvent accéder à vos dossiers. Celles non autorisées sont bloquées. Et, lorsqu'une appli tente de modifier un fichier dans un dossier protégé, Windows Defendeur vous envoie une notification. Le logiciel gère la liste des applications fiables mais vous pouvez aussi 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.

RAWPIXEL.COM/ADOBESTOCK