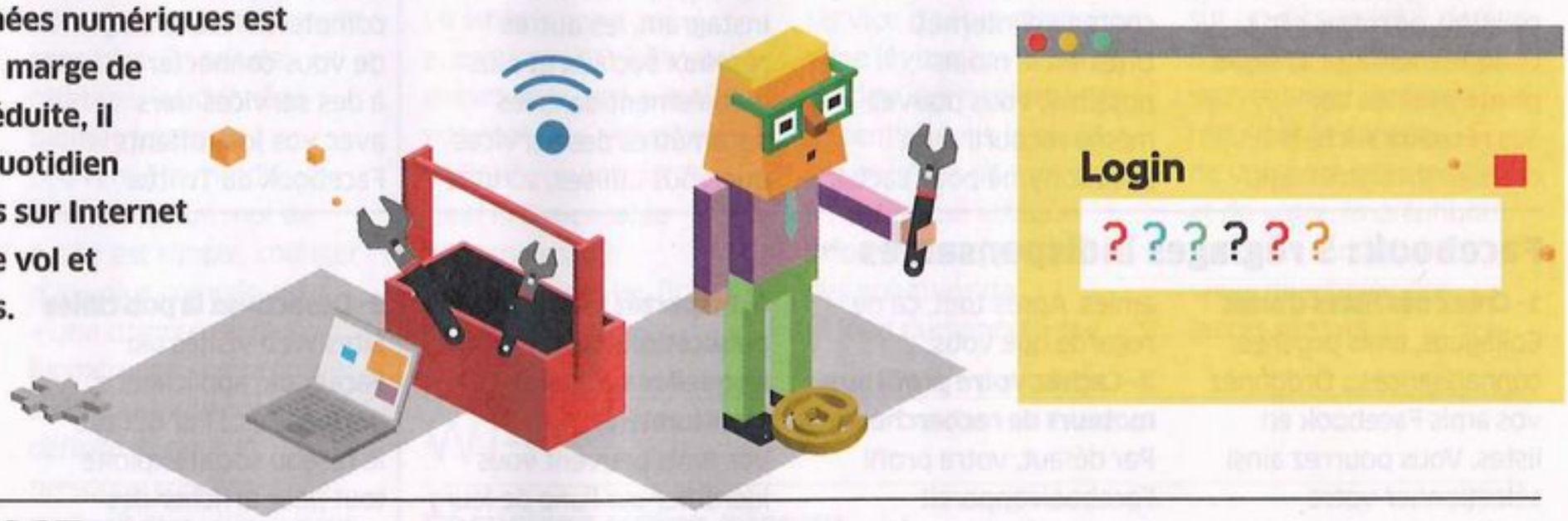
EN PRATIQUE

Comment protéger sa vie privée

La collecte de nos données numériques est inéluctable. Même si la marge de manœuvre est assez réduite, il est possible d'agir au quotidien pour réduire nos traces sur Internet et limiter les risques de vol et de piratage de données. Suivez le guide.



MOTS DE PASSE

Choisissez-les solides et uniques

Notre vie numérique est rythmée par la création de comptes avec identifiant et mot de passe. Les gérer est une corvée. Du coup, de nombreux utilisateurs choisissent le même mot de passe pour tous les services, et font en sorte qu'il ne soit pas trop difficile à mémoriser. Plus de la moitié des internautes utilisent les 25 mêmes mots de passe (parmi lesquels «password», «123321», «77777777», et... «google»)! 17% des internautes protègent leurs comptes avec «123456», mot de passe le plus fréquent en 2016 (Source: Keeper Security, 2017). Grossière erreur! La protection de ses données exige une certaine discipline.

COMMENT FAIRE

▸ **Variez** les mots de passe selon les services et choisissez les assez longs (8 à 12 caractères).

▸ **Bannissez** votre date de naissance ou les prénoms de vos proches. N'utilisez pas les mots du dictionnaire. Intégrez des caractères spéciaux, des chiffres, des lettres, en majuscule et en minuscule. Vous trouverez ci-dessous quelques astuces pour élaborer des mots de passe solides et mémorisables.

▸ **N'enregistrez pas** vos mots de passe dans le navigateur Internet (Internet Explorer, Firefox), surtout sur les ordinateurs professionnels ou publics.

▸ **N'envoyez pas** vos mots de passe par e-mail et effacez de votre boîte les messages de confirmation des sites sur lesquels vous venez de créer un compte.

▸ **Changez** de mot de passe tous les trois mois pour les sites sensibles (banque, e-mails).

Comment les construire

Plusieurs astuces permettent de créer des mots de passe mémorisables et déclinables selon les sites.

▸ **La méthode phonétique:** *«Je vais acheter 6 pommes de terre»* peut ainsi devenir *«JvAHT6pDT»*.

▸ **La méthode des premières lettres:** *«Mieux vaut prévenir que guérir»* qui donne, par exemple, *«M2vP_k_GéR»*.

▸ **Une information personnelle** comme *«Je me suis marié le 12 juin 1984»*, qui deviendrait *«J_M_Le12j84»*.

VOUS ÊTES EN PANNE D'INSPIRATION?

La Cnil propose un outil très pratique pour générer des mots de passe à la fois solides et faciles à retenir (https://www.cnil.fr/fr/generer-un-mot-de-passe-solide).

Deux preuves sinon rien

De nombreux sites proposent une «authentification à double facteur», qui ajoute un niveau de sécurité supplémentaire au simple mot de passe. Lorsque l'utilisateur se connecte, il saisit ses identifiants. Le site envoie ensuite un code sur son smartphone, à saisir pour valider l'identification. Apple, Google, Facebook, Twitter proposent cette option. Lorsqu'elle est disponible, activez-la.

Gestionnaires de mots de passe: peut-on leur faire confiance?

Un gestionnaire de mots de passe, comme Dashlane, KeePass ou LastPass, garde tous vos mots de passe en mémoire et vous permet d'y accéder en saisissant un mot de passe unique, complexe et connu de vous seul.

Pratiques, ces logiciels sont-ils sûrs? *«Toutes les informations sont encryptées côté utilisateur et la clé de cryptage qui permet d'accéder aux données du compte dépend du mot de passe maître. Rien de ce qui est acheminé vers nos serveurs n'est exploitable par personne»,* assure Thibault Behaghel, de LastPass. Les options avancées, comme la double authentification, sont payantes (abonnement premium à 12,99 €/an chez LastPass).

Optez dans tous les cas pour un opérateur sérieux. La sécurité offerte par KeePass, un logiciel opensource, a par exemple été approuvée par l'Anssi (Agence nationale de sécurité des systèmes d'information).

RÉSEAUX SOCIAUX

Restez discrets

Chaque information personnelle (opinion, religion, adresse, etc.), chaque message, chaque photo publiée sur les réseaux sociaux devient incontrôlable. Et il est difficile, ensuite, de faire disparaître un contenu d'Internet. Dites-en le moins possible; vous pouvez même recourir à un pseudonyme pour cacher votre identité. Sur Facebook, Twitter, Instagram, les autres réseaux sociaux et plus globalement dans les paramètres des services que vous utilisez, scrutez les paramètres de confidentialité de votre compte. Évitez, enfin, de vous connecter à des services tiers avec vos identifiants Facebook ou Twitter.

Facebook : 5 réglages indispensables

1- Créez des listes d'amis
Collègues, amis proches, connaissances... Ordonnez vos amis Facebook en listes. Vous pourrez ainsi sélectionner votre audience pour chacune de vos publications.

2- Masquez vos amis
Cachez aux autres les personnes avec lesquelles vous êtes amies. Après tout, ça ne regarde que vous.

3- Cachez votre profil aux moteurs de recherche
Par défaut, votre profil Facebook apparaît dans les résultats quand on cherche votre nom dans Google. Stop! Rendez-vous dans «Paramètres», puis «Confidentialité».

4- Inspectez les diverses publications dans lesquelles vous êtes mentionné(e)
Vos amis peuvent vous identifier sur l'une de leurs publications. Avant qu'elle n'apparaisse sur votre journal, approuvez-la. Allez sur «Paramètres» puis «Journal» et «Identification».

5- Désactivez la pub ciblée
Sites Web visités *via* Facebook, applications, partenaires... Par défaut, le réseau social exploite tout pour afficher des publicités ciblées sur vos pages. Restreignez ces accès si vous vous y opposez (dans le menu: «Paramètres» puis «Publicités»).

SMARTPHONE/TABLETTE

Stop au flicage

Votre smartphone est très curieux. Les géants du Web sont nichés à l'intérieur (*via* le système d'exploitation ou les applications), et il connaît tous vos déplacements puisque vous l'avez toujours avec vous. Quelques réglages permettent de limiter la collecte d'informations et de protéger vos données.

LES RÈGLES DE BASE

▸ **Définissez un mot de passe pour déverrouiller l'appareil.** Il constituera un premier rempart contre les intrusions dans votre vie privée en cas de perte ou de vol. Les smartphones Android offrent d'autres options de déverrouillage, comme un schéma (tracé d'un motif sur l'écran tactile) ou la reconnaissance de l'iris.

▸ **N'installez pas d'applications en dehors des boutiques App Store (iPhone) et Google Playstore (Android).** Certains piratent envoient par SMS des liens qui pointent vers des applications vérolées.

▸ **Dans les paramètres de confidentialité** (iPhone) ou dans les autorisations (Android), limitez les autorisations d'accès à votre localisation aux applications qui en ont vraiment besoin (navigation piétonne ou auto, par exemple).

▸ **Désactivez le ciblage publicitaire.** Sur un smartphone Android, rendez-vous dans «Les Paramètres Google», puis «Annonces». Sur un iPhone, «Confidentialité» puis «Publicité».

Allez aussi dans «Confidentialité» puis «Services de localisation» puis «Services système» et désactivez «Lieux fréquents».

▸ **Désactivez la mémorisation** des «Lieux fréquents» dans votre iPhone («Paramètres» puis «Confidentialité» puis «Services système») ou votre compte Google («Paramètres» puis «Suspendre l'historique des positions»).

Effacez vos données à distance

En cas de perte ou de vol de votre smartphone ou de votre tablette, vous serez soulagé de pouvoir l'effacer à distance. Pour cela, il est nécessaire de configurer cette option au préalable. Pour que le système fonctionne, l'appareil à effacer doit toutefois être allumé et connecté à Internet.

COMMENT FAIRE AVEC ANDROID
Installez l'application «Localiser mon appareil» sur votre smartphone. Connectez-vous avec les identifiants de votre compte Google. Depuis un navigateur Internet (sur ordinateur ou tablette), rendez-vous sur android.com/find (Android). Sélectionnez l'appareil concerné dans la colonne de gauche, puis cliquez sur «Activer verrouillage» et «Effacement».

COMMENT FAIRE AVEC IOS
L'application «Localiser» est installée par défaut. Connectez-vous avec vos identifiants Apple. Ensuite, depuis un navigateur Web, allez sur www.icloud.com. Repérez l'appareil à effacer puis cliquez sur «Effacer l'iPhone».

SÉCURITÉ

Oubliez la biométrie

Empreintes digitales, scanner de l'iris, reconnaissance faciale ou vocale... Les dispositifs d'identification par biométrie s'installent dans notre quotidien, pour déverrouiller notre smartphone ou accéder à notre lieu de travail. Les banques expérimentent également différents services, à l'image de La Banque postale, qui teste actuellement la reconnaissance vocale pour préremplir les formulaires de paiement en ligne. Mais l'iris, la voix et les empreintes digitales sont propres à chacun et constituent donc des données particulièrement sensibles. En cas de piratage, les données biométriques ne peuvent être modifiées: réinitialiser un mot de passe est simple, changer d'iris plus compliqué! *«Une caractéristique biométrique compromise a des conséquences définitives pour la personne concernée: elle pourrait être utilisée pour usurper son identité»*, prévient la Cnil. Sans doute est-il plus prudent de s'en passer...

Contre les virus et les malwares, installez un antivirus

Surfer sur Internet n'est pas sans danger. Des millions de fichiers malveillants circulent sur le Web, cherchant à pénétrer sur un maximum d'ordinateurs connectés. Ransomwares (ou «rançongiciels»), logiciels espions, malwares... Ces programmes sont utilisés par les pirates pour récupérer sur les ordinateurs des particuliers et des sociétés toutes sortes de données personnelles (coordonnées bancaires, mots de passe, adresses e-mail...) utilisées à des fins malveillantes ou pour prendre le contrôle de l'ordinateur à distance. Pour vous en prémunir, installez un bon antivirus. Nous les testons régulièrement (voir également notre test pp. 50-51).

PRÉVENTION

Sauvegardez vos données

Un disque dur en panne, un virus informatique, un smartphone qui prend l'eau et voilà vos documents, vos e-mails, vos contacts, vos photos définitivement perdus. Il est indispensable de sauvegarder régulièrement les fichiers stockés sur votre ordinateur sur un disque dur externe ou sur un service d'hébergement en ligne (évitez toutefois de stocker des papiers d'identité dans le cloud, ces services ne sont pas à l'abri d'une attaque informatique). Il existe des solutions de «cloud personnel» qui permettent d'accéder aux fichiers stockés chez soi, sur un disque NAS, depuis n'importe où. De même, sauvegardez de façon régulière le contenu de votre tablette tactile et de votre smartphone. Tous nos conseils sur www.quechoisir.org (accès gratuit).

WI-FI

Sécurisez votre réseau

Les pirates sont à l'affût des connexions faiblement sécurisées car, une fois connectés, ils peuvent vaquer tranquillement à leurs occupations illicites (téléchargement illégal, interception d'informations, piratage de comptes...). Chacun de nous est responsable devant la loi des activités liées à sa connexion Internet. Pour sécuriser votre réseau Wi-Fi, commencez par le cacher. De cette façon, il n'apparaîtra plus dans la liste des réseaux disponibles. Pour cela, rendez-vous dans la section Wi-Fi des paramètres de votre box et désactivez la diffusion du «SSID». Ensuite, changez le mot de passe par défaut. Enfin, choisissez l'option de chiffrement la plus complexe (en passant du WEP au WPA2).

COMMENT FAIRE

Pour accéder à l'interface de gestion de votre box, ouvrez votre navigateur (Internet Explorer, Mozilla....) et dans la barre d'adresse, saisissez: http://livebox/ ou 192.168.1.1 (Orange); http://gestionbbox.lan ou 192.168.1.254 (Bouygues Telecom); mafreebox.freebox.fr (Free); http://monmodem ou http://192.168.0.1 (SFR).

PUBLICITÉ EN LIGNE

Bientôt moins intrusive, mais toujours curieuse

Entre les fenêtres intempestives (pop-up), les bandeaux fixes et les vidéos à lecture automatique, la navigation sur Internet vire au cauchemar. Pour limiter la gêne, vous pouvez installer un bloqueur, comme Adblock (pubs), Disconnect ou Ghostery (antitraceurs). Preuve de l'agacement qu'elles suscitent, un quart des internautes ont installé un bloqueur de publicités, selon l'Institut CSA. Cette colère n'a pas échappé à Google qui, dès 2018, bloquera automatiquement dans son navigateur Chrome les formats publicitaires les plus détestés. Cette initiative n'a rien de philanthropique. Elle vise plutôt à couper l'herbe sous le pied des «adblockers». Le plus célèbre d'entre eux, AdBlock Plus, monnaye en effet la possibilité, pour les grands groupes, d'afficher quand même les publicités qu'ils considèrent «acceptables» selon leurs propres règles. En filtrant lui-même les pubs, Google s'assure la sympathie des internautes qui, en adoptant Chrome comme navigateur, continueront à lui en apprendre beaucoup sur leurs habitudes de consommation.

MOTEURS DE RECHERCHE

Au placard, Google !

Google réalise plus de 87% de son chiffre d'affaires grâce à la publicité. Nos données numériques, qui servent au profilage des consommateurs, constituent sa matière première. Lorsque nous cherchons des informations sur son moteur de recherche, nous sommes à la fois fournisseurs (l'historique de recherche en dit long sur nos centres d'intérêt) et clients (les premiers liens qui s'affichent sont des publicités). Certains moteurs de recherche alternatifs assurent qu'ils protègent notre vie privée. C'est le cas de l'américain DuckDuckGo ou du français Qwant. Ce dernier est partenaire de Microsoft Bing pour les publicités (qui demeurent sa seule source de revenus), mais assure qu'il ne trace pas les internautes. Qwant confesse aussi qu'il complète les résultats de recherche avec ceux de Bing, notamment pour les images (lorsque, sur Google, on limite sa recherche sur « Images », ndlr), en attendant que *« tout le Web soit parfaitement indexé »*. Le moteur reste malgré tout une alternative intéressante (lire aussi notre enquête sur les moteurs de recherche alternatifs, *QC* n° 557). À titre de comparaison, un internaute rapporte en moyenne 12 € par an à Qwant, et jusqu'à 100 € par an à Google, grâce au ciblage publicitaire !

MESSAGERIE

Créez plusieurs adresses e-mails

Pour ne pas rater un message des impôts ou de la Sécu noyé parmi les publicités et les spams, créez plusieurs adresses e-mails. Un compte pour vos correspondances « sérieuses » (avec les proches, l'administration, vos contacts du travail, vos loisirs), un autre pour les réseaux sociaux et les forums, et un dernier pour les tiers sans importance (cartes de fidélité, jeux, etc.).

NAVIGATION INTERNET

Halte au pistage

Lorsque vous naviguez sur Internet, vous êtes suivis à la trace. Un petit tour dans les options de votre navigateur (Internet Explorer, Mozilla Firefox, Chrome, Safari) permet de verrouiller quelques paramètres. D'abord, activez l'option « Ne pas me suivre ». Les sites visités seront alertés que vous ne souhaitez pas être pisté (rien ne les contraint à respecter ce choix). Ensuite, bloquez les cookies « tiers », qui ne sont pas indispensables à la bonne navigation. Certains sites demandent au navigateur où vous êtes. Leur argument est de livrer une information plus précise (les restaurants autour de vous lorsque vous voulez manger une pizza, par exemple). Mais cette donnée est surtout précieuse pour les publicitaires. Dans les paramètres, vous pouvez interdire à votre navigateur de vous géolocaliser. Bloquer les « pop-up » (fenêtres intempestives) vous épargnera l'affichage de nombreuses publicités. Enfin, lorsque vous utilisez un ordinateur autre que le vôtre, ouvrez une fenêtre de « Navigation privée ». Votre historique de navigation ne sera pas enregistré, ni vos mots de passe.

COMMENT FAIRE

Accédez aux paramètres de confidentialité et de sécurité de votre navigateur :

▸ **FIREFOX :** « Outils » puis menus « Vie privée et Sécurité ».

▸ **INTERNET EXPLORER :** « Réglages » puis « Sécurité » (pour activer « Ne pas me suivre ») ; « Outils » puis « Options Internet » puis « Confidentialité ».

▸ **CHROME :** « Réglages » puis « Paramètres » puis « Afficher les paramètres avancés ».

MORT NUMÉRIQUE

Exprimez vos dernières volontés

La loi pour une République numérique d'octobre 2016 instaure le droit de décider du sort de ses données en cas de décès. Chaque service doit donc permettre aux utilisateurs d'établir un « testament numérique ». Le décret d'application n'est pas encore publié, mais plusieurs plateformes ont pris les devants. Dans les paramètres de votre compte Facebook, par exemple, il est possible de désigner un contact légataire qui gérera votre compte après votre décès, ou d'indiquer dès à présent que vous souhaitez que votre compte soit supprimé. Il faudra bien sûr que Facebook ait été prévenu de votre disparition (la démarche est accessible en ligne). Google a également mis en place un « Gestionnaire de compte inactif » qui permet d'alerter jusqu'à 10 proches ou de supprimer votre compte si vous ne vous êtes pas connecté depuis 3, 6, 9, 12 ou 18 mois.

Retrouvez l'intégralité du tchat sur http://ufcqc.link/tchat563

DONNÉES PERSONNELLES • VOS QUESTIONS/NOS RÉPONSES

Collecte, exploitation, protection des données numériques... Des concepts un peu vagues dont, souvent, les enjeux sont mal perçus. Certains consommateurs assez aguerris semblent, au contraire, déjà en résistance face à Google et aux autres géants du Web.

Les questions qui suivent sont issues de notre tchat en direct organisé le 6 avril 2017, animé par Camille Gruhier (journaliste), avec Karine de Crescenzo (responsable des relations institutionnelles) et Justine Massera (juriste).

L'exploitation des données personnelles représente-t-elle un danger dans un état démocratique? JEAN-JOSEPH B. ET YVELINE M.

QC L'exploitation marchande des données constitue la pierre angulaire de l'économie numérique. Notre état démocratique est aussi un état libéral, il est important d'éviter les dérives. Notre cadre légal est l'un des plus restrictifs au monde, protégeons-le pour que le consommateur ne soit jamais dépossédé de son droit fondamental à la vie privée.

Quelles données sont considérées comme personnelles par la loi? BRIDEAL

QC Toute information relative à une personne physique identifiée, ou qui peut être identifiée, directement ou indirectement constitue une donnée personnelle. Par exemple un nom, un prénom, un âge, un code postal, un numéro de téléphone ou de Sécurité sociale. Prises isolément, ces données ne parlent pas toujours, mais il suffit de les croiser pour identifier la personne.

La Loi informatique et libertés n'est-elle pas un peu désuète? BRIGITTE T.

QC La Loi informatique et libertés pose le cadre juridique qui permet aux entreprises de collecter et traiter des données pour fournir un service au consommateur. Elle garantit aussi un certain nombre de droits à ce dernier (consentement à la collecte, droit d'accès, de s'opposer, de rectifier). Ce texte un peu obsolète, il est vrai, est renforcé par la loi pour une République numérique, adoptée récemment, et par le Règlement européen sur la protection des données personnelles, qui entrera en vigueur en mai 2018. Ces deux nouvelles lois érigent en principe fondamental la maîtrise par l'individu de ces données pendant sa vie et après sa mort.

Qu'advient-il de nos données quand on nous demande notre nom et date de naissance dans un magasin, pour obtenir des avantages ou une carte fidélité? DÉDÉ

QC Cette question illustre le fait que la collecte de données personnelles ne date pas du numérique. La loi informatique, qui encadre leur collecte et leur protection, date de 1978! Les sociétés les récupèrent dans la vie réelle dès qu'elles le peuvent. Elles constituent ainsi des fichiers clients et des bases de données leur permettant de connaître nos habitudes et nos goûts pour nous proposer des offres ciblées.

Est-il illégal de donner de faux renseignements si un site demande des données personnelles? KHENTY ET LAHCEN

QC Livrer une fausse information n'est pas problématique à partir du moment où cette information n'est pas nécessaire à la fourniture du service ou non requise lors d'une déclaration officielle (impôts, Sécurité sociale, vérification d'identité). Attention toutefois aux cas où cette donnée obligatoire vous ouvre un droit particulier, par exemple, une promotion pour les moins de 25 ans. Un faux renseignement pourrait entraîner votre responsabilité contractuelle (fraude).

Facebook m'oblige à lui envoyer une pièce d'identité pour accéder à mon compte. Est-ce légal? SYLVIE B.

QC Depuis fin 2015, Facebook impose la présentation d'une identité conforme à celle utilisée dans la vraie vie. Il peut être amené à vous demander de justifier votre identité par une pièce d'identité officielle (carte d'identité, carte d'électeur, permis de conduire, etc.). La Cnil (Commission nationale de l'informatique et des libertés) n'y voit pas d'inconvénient.

Les cookies sont-ils bons ou mauvais? GRILLET

QC Les cookies sont parfois bons, parfois mauvais... Ils permettent, par exemple, de conserver les articles mis dans un panier lors de vos achats en ligne. Mais ils donnent aussi de nombreux renseignements sur votre navigation, lesquels serviront à cibler la publicité qui s'affichera par la suite sur votre écran.

Certains sites tels qu'Amazon gardent en mémoire le numéro de nos cartes bancaires. Ces données sont-elles en sécurité? FRANÇOISE S.

QC Une fois le paiement effectué, les sites marchands n'ont pas le droit de conserver votre numéro de carte bancaire sans votre accord (ils peuvent toutefois le garder pendant 15 mois, en cas de contestation concernant la transaction). Le plus souvent, ils recueillent ce consentement grâce à une petite case à cocher (il n'est pas rare qu'elle soit précochée par défaut, ce qui est en théorie interdit). La Cnil exige que ces données bancaires soient cryptées par un algorithme de chiffrement «fort». Les accès et les liaisons au site marchand doivent être également sécurisés.

Comment se passer des logiciels «imposés» directement ou indirectement du genre Google? GILLES S.

QC Il existe des dizaines de services alternatifs à ceux de Google, dans tous les domaines. Citons OpenMailBox pour remplacer Gmail, OpenStreetMaps pour remplacer Google Maps ou encore Qwant pour remplacer le moteur de recherche. Framasoft, un réseau qui promeut les logiciels libres, propose une bibliothèque très fournie dans le cadre de son initiative «Degooglisons Internet».

Les objets connectés, dont nous n'avons pas besoin, ne vont-ils pas collecter encore plus de données pour le bénéfice des fabricants? GILLES S.

QC Il est vrai que la mode des objets connectés part un peu dans tous les sens. Et oui, bien sûr, ils sont susceptibles de collecter des données... Les bracelets de bien-être, par exemple, en savent beaucoup sur votre activité quotidienne. Et ces données pourraient intéresser des assureurs. C'est inquiétant, mais *Que Choisir* veille au grain!