SÉBASTIEN ERMACORE

SYLVAIN PILPAY

INTERNET
SURFEZ EN SÉCURITÉ

30 ANS DU WEB
1989-2019

Protéger son ordinateur et sa connexion, lutter contre les spams et les virus, surfer tranquille sur les réseaux sociaux

Éditions EYROLLES

INTERNET **SURFEZ EN SÉCURITÉ**

Le Web a fêté son 30e anniversaire en mars 2019 ! Aujourd'hui, plus de 57 millions de Français surfent régulièrement sur Internet. Près de 60 % d'entre eux ont un compte sur les réseaux sociaux. Dans le même temps, les usages du e-commerce explosent avec 37,5 millions des Français qui ont acheté en ligne en 2018.

Pour s'y retrouver, cet ouvrage clair et concis a pour objectif d'apprendre à surfer en toute sécurité en sécurisant sa connexion à Internet (box), en protégeant ses données personnelles sur les réseaux sociaux, en apprenant à se protéger contre les virus, etc. S'adressant aux utilisateurs habitués comme aux grands néophytes, vous y découvrirez tout ce qui vous protégera pendant votre navigation.

Agrémenté de nombreuses illustrations et à jour des dernières législations en vigueur, cet ouvrage vous accompagne de façon progressive dans la maîtrise des outils du quotidien Internet, tels que le navigateur ou la messagerie électronique et vous propose également les principales règles de bonne conduite et de sécurité vis à vis des virus, des spams et des dangers liés à l'utilisation des réseaux sociaux.

À QUI S'ADRESSE CET OUVRAGE ?

- À toutes celles et tous ceux qui souhaitent comprendre et maîtriser un peu mieux les principaux outils de communication sur Internet.
- Aux associations et aux familles qui pourront utiliser l'ouvrage pour sensibiliser sur les dangers d'Internet aujourd'hui.

SOMMAIRE

LES AUTEURS

SÉBASTIEN ERMACORE est passé maître dans l'art de l'administration des systèmes d'information et du développement d'applications web. Plongé très jeune dans une marmite Linux/Unix, son langage, certes binaire, se compose de balises, de caractères spéciaux, de lignes de codes et de commandes illisibles. Mais derrière cette carapace technique effrayante, il a tenu à développer depuis de nombreuses années des formations pour des publics divers et variés, experts techniques de grandes entreprises, étudiants en apprentissage ou personnes en reconversion professionnelle.

SYLVAIN PILPAY est né un crayon à la main et n'a eu de cesse d'explorer les outils lui permettant d'éviter l'usage du taille-crayon, et donc de laisser des copeaux de bois partout où il passait. Il a vu naître et se développer les logiciels de graphisme et s'est très vite passionné pour la suite Adobe. Infographiste et webmestre, il s'est spécialisé dans la conception de chartes graphiques, logos, visuels et la conception de sites Internet réalisés avec le minimum de lignes de codes. Il enseigne Photoshop, Illustrator, InDesign et Joomla! depuis plusieurs années maintenant pour tous publics.

SÉBASTIEN ERMACORE

SYLVAIN PILPAY

INTERNET
SURFEZ EN SÉCURITÉ

Protéger son ordinateur et sa connexion, lutter contre les spams et les virus, surfer tranquille sur les réseaux sociaux

Éditions EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Conception maquette et mise en pages : Soft Office

 ISBN : 978-2-212-67740-9

Remerciements

Merci à toi Sylvain, pour ta patience et ton abnégation. Toujours constructif, toujours inventif, je suis très honoré que tu aies accepté de mettre ton talent à disposition de ce projet, qui ne serait pas le même sans toi !

Merci à ma petite famille, qui m'accompagne sans aucun doute sur toutes mes idées folles les unes après les autres.

Sébastien Ermacore

Sébastien, tu as aimé mes petits Miquets et m'as poussé à en faire plein dans ce livre, avec des idées souvent incroyables. La réalisation de ce projet avec toi m'a beaucoup apporté, et surtout beaucoup de plaisir ! Pour cela, je t'en remercie.

Chaque dessin est envoyé pour approbation à ma femme et à ma fille. Et j'attends un retour avec la patience d'un chat qui se brûle. Et à chaque fois, ce retour est souvent bienveillant, parfois sévère. Merci à vous deux.

Sylvain Pilpay

Remerciements particuliers à René qui a bien voulu interpréter le Virus et les autres créatures de cet ouvrage. Aucune créature ni aucun animalcule n'ont été blessés durant la réalisation de cet ouvrage.

Kory Pilpay est étudiante en animation 3D, dessinatrice compulsive et conseillère démunie de tout sentiment. Elle a apporté un regard critique constant sur la réalisation de cet ouvrage et apporté sa plume dans quelques croquis délicats. Merci à elle.

Table des matières

Chapitre 1

Sécuriser son ordinateur et sa connexion Internet

Vous souhaitez surfer en sécurité ? Quelques notions fondamentales vous permettent de le faire simplement ! Dans ce chapitre, nous aborderons le schéma classique d'une connexion Internet et les actions nécessaires pour sécuriser facilement votre box Internet et votre ordinateur.

Sommaire

Le fonctionnement d'une connexion Internet

Définition Qu'est-ce qu'Internet ?

Réseau reliant des ordinateurs. Dans une grande majorité des cas, les ordinateurs sont reliés entre eux grâce à des câbles de connexion, à la manière des terminaux de téléphone. Ces câbles de connexion parcourent le monde entier et peuvent être assez légers pour une liaison proche (connecteurs RJ45) ou énormes et très volumineux, pour une liaison lointaine (les *backbones* de fibres optiques, épines dorsales de l'océan Atlantique par exemple).

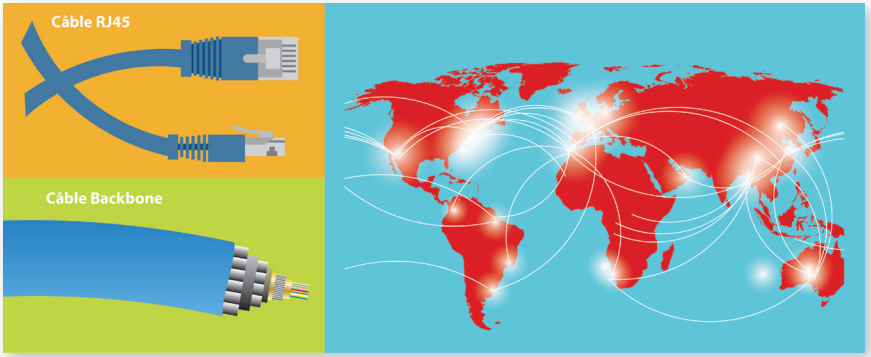
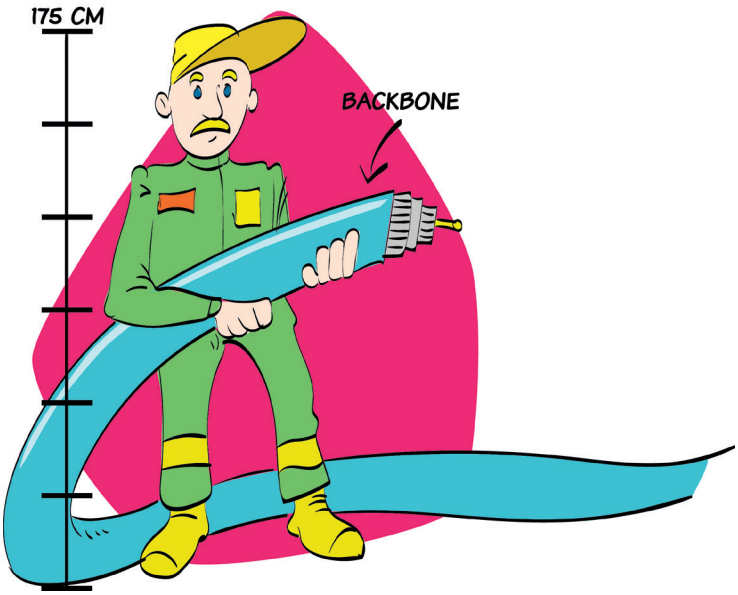


Fig. 1-1 *Les câbles RJ45, le plan de coupe d'un backbone atlantique, la carte mondiale des backbones.*



Il est également possible de faire communiquer des terminaux distants avec les ondes, que ce soit sur grande distance (GSM, satellite) ou sur petite distance (Wi-Fi, Bluetooth). Ainsi en utilisant ces différents types de support de communication (câbles et/ou ondes) — y compris en les cumulant — il est possible de connecter des ordinateurs d'un bout à l'autre de la planète.

La figure 1-2 montre Sylvain envoyant un message à Sébastien via différents réseaux de communication :

- les ondes électromagnétiques, avec aujourd'hui la 4G et demain la 5G ;
- les câbles et les fibres optiques.

Avec ces supports de communication, le message de Sylvain émis depuis son téléphone peut parcourir une très grande distance physique avant d'atteindre l'ordinateur de Sébastien sans se perdre.

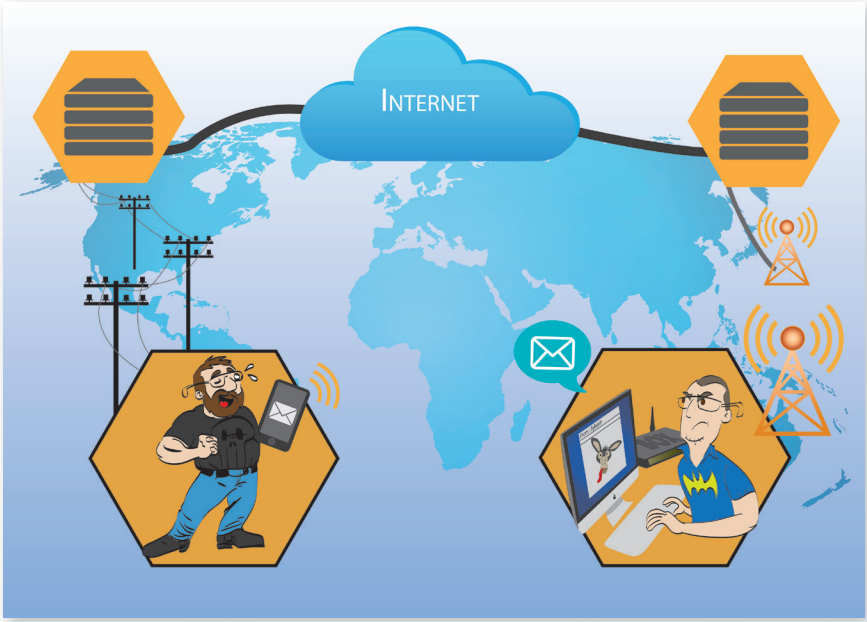


Fig. 1–2 *Sylvain envoie un message à Sébastien via différents réseaux de communication.*

Ce phénomène est assuré grâce à quelques principes réseaux fondamentaux. Notamment le fait qu'un ordinateur ou terminal connecté à Internet est identifié de manière unique par son identifiant : l'adresse IP. Le choix du mot « adresse » n'est pas innocent, en effet, cet identifiant fonctionne de la même manière que votre boîte aux lettres physique. Par exemple l'adresse « 17, rue des Merisiers, 75013 PARIS France » est unique sur la planète !

Les adresses identifiant un ordinateur de manière unique sont nommées « des adresses IP » car elles s'appuient sur le protocole réseau IP (*Internet Protocol*) et sont légèrement plus indigestes à déchiffrer que celles du courrier postal, par exemple 150.17.155.12 est unique au monde, ou encore 2001:0db8:0000:85a3:0000:0000:ac1f:8001 !

Heureusement, nous n'avons pas à les retenir, les machines le font pour nous.

Lorsque le message de Sylvain arrive chez Sébastien, il doit passer par l'équivalent de sa boîte aux lettres, qui est en réalité son boîtier de connexion. Si vous êtes connectés à Internet, vous louez probablement cette fameuse « box Internet » à votre opérateur préféré (Orange, SFR, Bouygues, etc). À cette box est effectivement associée une adresse IP unique. Vous ne la choisissez pas, l'opérateur en charge de votre ligne est responsable de votre adresse IP et votre voisin n'aura évidemment pas la même que la vôtre !

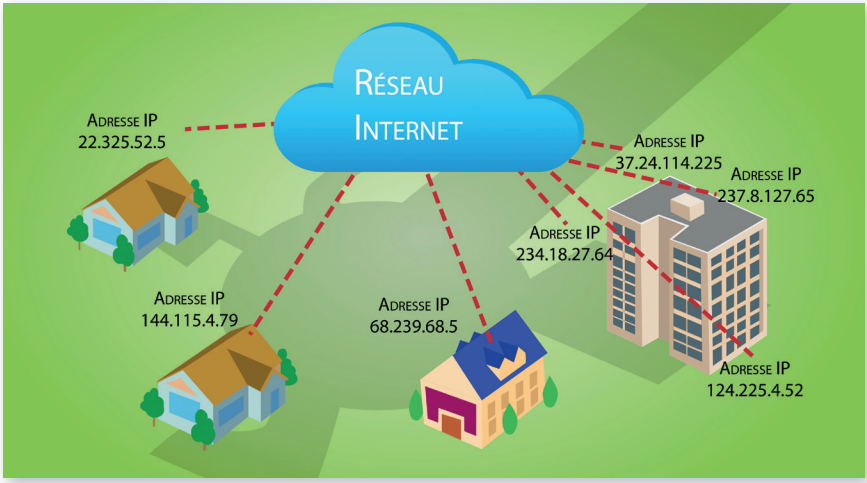


Fig. 1-3 *Représentation des adresses IP publiques*

La figure 1-3 montre quelques habitations et leurs adresses IP uniques au monde respectives.

En règle générale, votre boîte aux lettres physique est disposée à l'entrée de votre habitation (hall de l'immeuble, portail d'entrée, mur donnant sur la rue, etc.). Ainsi le facteur n'est pas obligé de rentrer chez vous pour déposer votre courrier.

Si votre box Internet est souvent rangée à l'intérieur de votre domicile, il est très important de comprendre qu'elle joue aussi le rôle de portail Internet.

Fig. 1-4 *Schéma du réseau domestique*

En effet, tous les équipements connectés de votre domicile souhaitant émettre un message sur Internet devront obligatoirement passer par la box et inversement, tout message à destination d'un équipement connecté chez vous passera par votre box avant d'entrer sur votre réseau.

C'est pourquoi il est très important de protéger cet accès.

Sécuriser sa box Internet

Avec une connexion filaire (via un câble Ethernet), il est tout de même assez difficile de s'introduire sur votre réseau domestique, car il faudrait pour cela entrer physiquement dans l'habitation ! La faille serait donc sur votre porte d'entrée ou autre, mais c'est une tout autre problématique. En revanche, la box Internet propose également de connecter votre réseau domestique via les ondes et le Wi-Fi. Or, ces ondes dépassent le périmètre des murs et sont donc accessibles à l'extérieur de l'habitation.

Une personne disposant d'un périphérique Wi-Fi en dehors de votre domicile (la maison mitoyenne, ou l'appartement du dessus) peut se connecter sur votre box et éventuellement :

- inspecter tous les équipements de votre réseau local, et chercher à pirater vos données ;
- utiliser votre ligne Internet à des fins malveillantes, téléchargements illégaux, envoi de messages spams, etc.

Par ailleurs, la loi Hadopi prévoit une amende et une coupure de l'accès Internet pour les connexions non sécurisées !

Il existe quatre grands principes pour protéger votre box Internet :

- sécuriser le mot de passe de l'interface d'administration ;
- mettre en place le filtrage du matériel ;
- dissimuler le signal ;
- crypter les transmissions.

Le montant de la contravention Hadopi

La contravention pour négligence caractérisée est punissable d'une amende de cinquième classe pouvant aller jusqu'à 1500 euros. Cette amende peut aller jusqu'à 3750 euros en cas de réabonnement chez un autre fournisseur d'accès.

→ *Source : http://www.la-loi-hadopi.fr/risques-hadopi/25-sanction-hadopi.html*

Principe #1 changer le mot de passe admin

Le mot de passe de l'interface d'administration est souvent initialisé de manière peu sécurisée à la livraison de la box. Sur les anciennes versions, c'était « admin » par défaut. Sur les nouvelles versions c'est souvent les 8 premiers/derniers caractères du numéro de série de la box. Quoi qu'il en soit, il est important de changer ce mot de passe. Pour cela, vous devez :

- vous connecter avec un navigateur sur l'interface d'administration de la box, en saisissant l'adresse suivante http://192.168.1.1 dans la barre d'adresse ;
- saisir une première fois le mot de passe admin par défaut pour accéder à l'onglet administration ;
- changer le mot de passe admin par défaut.

La figure 1-5 montre l'exemple de l'interface d'administration d'une box Orange.

Avec cette première action, vous protégez l'accès à l'interface d'administration de votre box, en cas d'intrusion sur votre ligne Internet. C'est important !

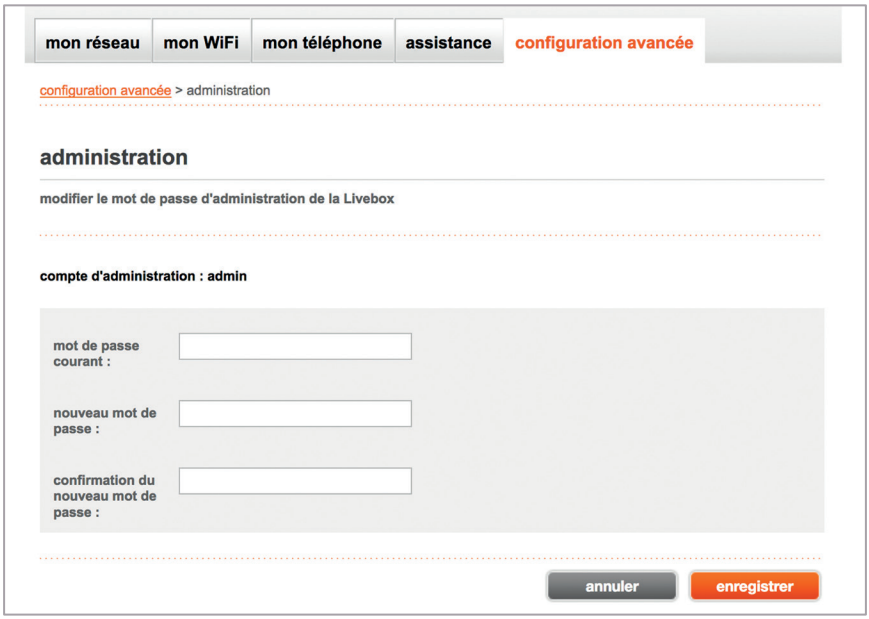


Fig. 1-5 *Changer le mot de passe admin sur une box Orange*

Principe #2 le filtrage du matériel

La mise en place d'un filtrage du matériel permet d'indiquer à votre box la liste des équipements informatiques (PC, tablettes, téléphones, etc.) autorisés à se connecter en Wi-Fi. Ainsi un individu situé à l'extérieur de votre domicile qui parviendrait à capter votre signal Wi-Fi ne pourrait pas se connecter, car votre box ne reconnaîtrait pas son équipement.

Les équipements informatiques connectés à un réseau local sont reconnus grâce à un autre identifiant unique, nommé également par le terme adresse : il s'agit des « adresses MAC » (pour *Media Access Control*). À ne pas confondre

avec les adresses IP évoquées précédemment, les adresses MAC sont écrites en hexadécimal sur 6 octets, par exemple 5E:FF:56:A2:AF:15. C'est très indigeste également, mais encore une fois, nous les humains n'avons pas besoin de les retenir, fort heureusement !

Il est donc possible d'indiquer à votre box Internet de ne connecter que les équipements que vous lui indiquez, en renseignant les adresses MAC de ces équipements dans son tableau de filtrage. Cette procédure s'effectue depuis l'interface d'administration de la box (d'où l'intérêt de protéger son accès par un mot de passe, comme détaillé dans le principe #1 ci-dessus), dans le menu Wi-Fi avancé.

Par défaut, le filtrage du matériel est souvent désactivé.

Fig. 1-6 *Option filtrage du matériel désactivée*

Une fois le filtrage activé, l'interface vous propose déjà la liste des équipements connectés à votre Wi-Fi, il suffit juste d'accepter ceux que vous reconnaissez.

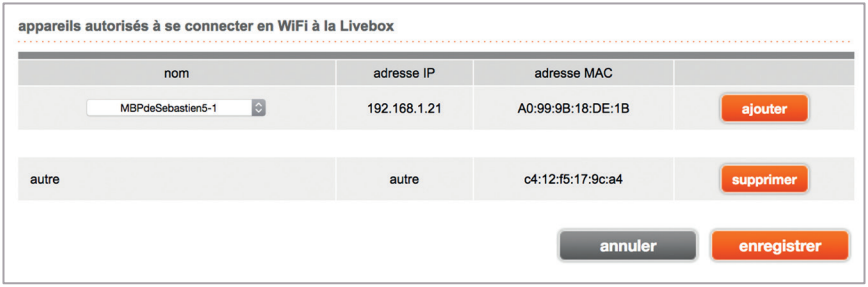


Fig. 1-7 *Option filtrage du matériel activée*