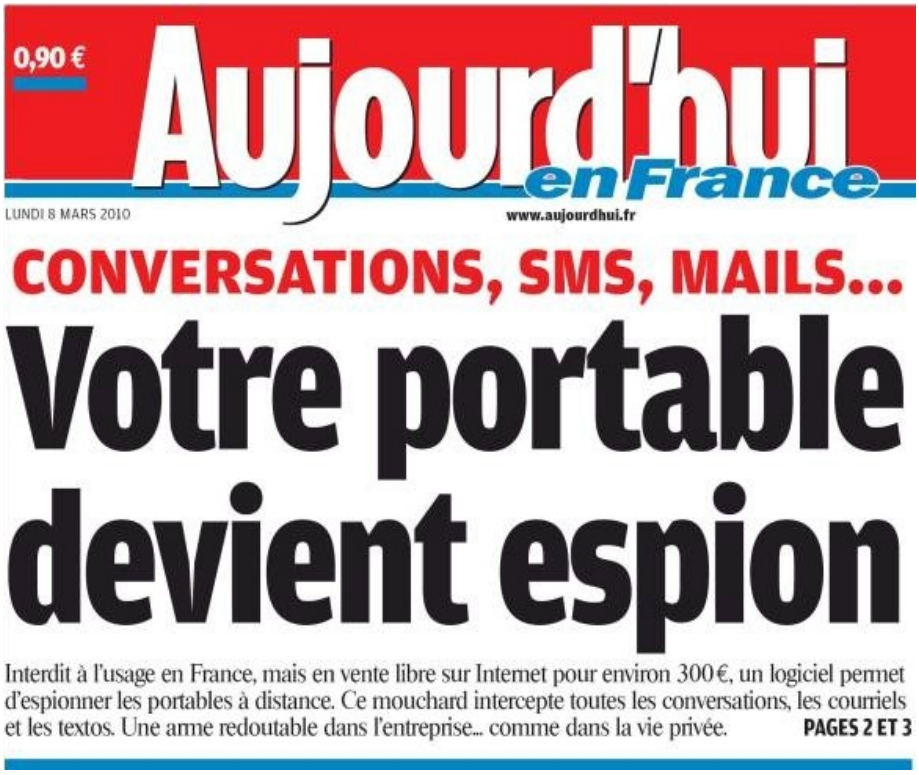
PETIT MANUEL DE CONTRE-ESPIONNAGE INFORMATIQUE

LE 24 MAI 2010 ***JEAN MARC MANACH***

GPS, téléphones portables, logiciels espions: les outils de la surveillance se démocratisent. Conseils utiles pour s'en protéger.

Autrefois réservés aux seuls services secrets, les outils et technologies de surveillance, GPS, téléphones et logiciels espions, se "*démocratisent*" au point que, suite à un reportage de M6, **Petits espionnages en famille**, montrant comment de plus en plus de gens espionneraient les téléphones portables et ordinateurs de leur futurs (ou ex-) femmes (ou maris), enfants, nounous, Le Parisien/Aujourd'hui en France faisait sa "une", début 2010, sur la question (**Votre portable devient espion**), tout en expliquant qu'espionner les téléphones portables était devenu "***un jeu d'enfant***" (à toutes fins utiles, en France, leur commercialisation, mais également leur simple détention, n'en est pas moins punie d'un an de prison et de 45 000 euros d'amende).



0,90 €

Aujourd'hui en France

LUNDI 8 MARS 2010 www.aujourdhui.fr

CONVERSATIONS, SMS, MAILS...

Votre portable devient espion

Interdit à l'usage en France, mais en vente libre sur Internet pour environ 300 €, un logiciel permet d'espionner les portables à distance. Ce mouchard intercepte toutes les conversations, les courriels et les textos. Une arme redoutable dans l'entreprise... comme dans la vie privée. PAGES 2 ET 3

Nombreux sont les médias à s'être penchés sur la question, de façon souvent quelque peu sensationnaliste. Aucun n'a dans le même temps cherché à expliquer comment l'on pouvait s'en protéger.

Le fait est que, et aussi paradoxal que cela puisse être, **la CNIL explique bien, par exemple, comment nous sommes tracés sur le Net… mais sans jamais nous expliquer comment s'en protéger**. Et si ces techniques d'espionnage existent depuis des années, force est de constater que jamais les autorités n'avaient cherché, jusque-là, à expliquer aux gens comment s'en protéger (voir, à ce titre, "**Internet : quand l'Etat ne nous protège pas**").

Or, il se trouve que **deux agences, liées aux services de renseignement français, viennent précisément de publier coup sur coup deux guides destinés à nous aider à sécuriser nos ordinateurs et téléphones portables**, et garantir la confidentialité de nos télécommunications.

Initialement destinés à tous ceux qui, patrons, chercheurs, cadres supérieurs, négociateurs, peuvent, du fait de l'espionnage industriel, voir leurs communications surveillées, leur lecture s'avère également très instructive pour tous ceux qui chercheraient à se protéger de l'espionnite aïgue de leurs parents, conjoints, employeurs ou collègues.

Une lecture que goûteront également probablement ceux qui, inquiets des projets de surveillance de l'internet prévus par l'**Hadopi**, la **Loppsi**, l'**ACTA**, ou encore par les **pouvoirs accrus** confiés aux forces de police et services de renseignement, sont aujourd'hui soucieux de protéger leur vie privée, et leurs libertés.

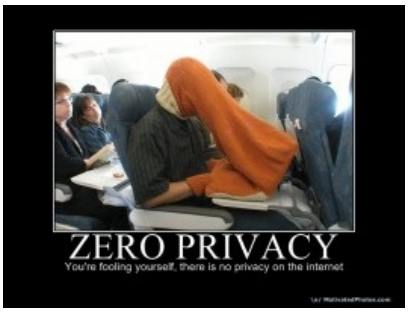
Alors que Reporters Sans Frontières célébrait récemment la **journée mondiale contre la cyber-censure** (près de cent vingt blogueurs, internautes et cyber-dissidents **sont en prison**, en Chine, au Viêt-nam ou en Iran notamment), il n'est en effet pas anodin de noter que les démocraties aussi, **surveillent**, et **censurent l'internet**…

A lire en complément du mode d'emploi que m'avait commandé, l'an passé, une revue du CNRS : **Comment contourner la cybersurveillance**…

Vous êtes en état d'interception : toutes vos télécommunications pourront être retenues contre vous

En août 2008, le département de la sécurité intérieure (DHS) américain annonçait que les ordinateurs portables de toute personne passant par les Etats-Unis pourraient désormais être saisis :

> ***La police des frontières américaines pourra désormais saisir le matériel électronique des voyageurs pour "examiner et analyser l'information transportée par un individu qui tente d'entrer, de réentrer, de partir, de passer en transit ou qui réside aux Etats-Unis", même si aucun soupçon ne pèse sur l'individu ou les informations qu'il transporte.***



Les fédéraux américains peuvent ainsi "*détenir les documents et les équipements électroniques, pour une période raisonnable afin de pouvoir faire une recherche approfondie*" sur place ou en envoyant l'ordinateur à des spécialistes.

Critiqué de toutes parts, le DHS expliqua que cela lui permettait de lutter contre le terrorisme, la pédo-pornographie, mais aussi le vol de propriété intellectuelle, et **précisa** que la pratique n'avait rien de nouveau, que ses agents le faisaient depuis bien longtemps :

> ***"Depuis la fondation de la République, nous avons eu la capacité de faire des recherches aux frontières afin d'éviter l'entrée dans le pays d'individus et de produits dangereux. Au 21ème siècle, la plus dangereuse des contrebandes est souvent contenue dans les médias électroniques et pas sur du papier. L'ère des dossiers de papiers et des microfiches est révolu."***

Les autorités françaises, elles, y voient quand même un léger petit problème. Sans pointer explicitement du doigt les USA (d'autant que ce genre de fouille approfondie n'est pas l'apanage des Etats-Unis), les deux modes d'emploi, publiés en décembre et janvier 2010, expliquent comment, précisément, réduire les risques, et protéger ses données, dès lors que l'on voyage ou part en mission avec un téléphone mobile, un assistant personnel ou un ordinateur portable.

De fait, la guerre économique, et l'espionnage industriel, sont une réalité souvent mal perçue par ceux qui, pourtant, peuvent en faire les frais. En 2005, les Renseignements Généraux **estimaient** ainsi qu'"*une société sur quatre est ou a été touchée par l'espionnage industriel*".

En 2009, une "*note blanche*" de la Direction centrale du renseignement intérieur (DCRI) **révélait** que "*près de 3000 firmes françaises ont été victimes de très nombreuses "actions d'ingérences économiques", destinées à leur voler leurs secrets de fabrication, à déstabiliser leur direction ou à gêner le lancement de nouveaux produits*" entre 2006 et 2008.

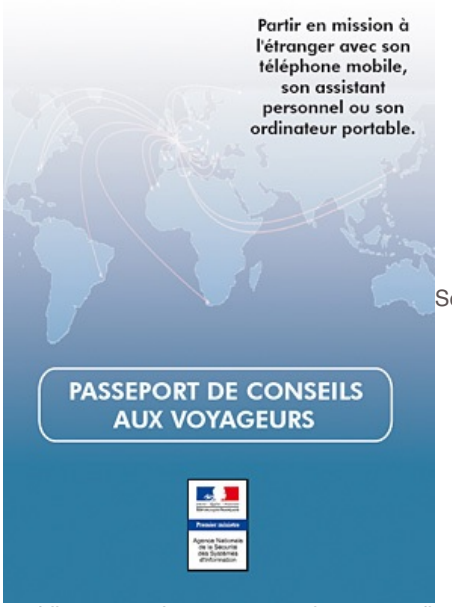
Evitez, SVP, d'utiliser un ordinateur…

> ***"Seul un ordinateur éteint, enfermé dans un coffre-fort et enterré six pieds sous terre dans un endroit tenu secret peut être considéré comme sécurisé, et encore."***
> ***– Bruce Schneier, expert mondialement réputé pour ce qui est des questions de sécurité informatique.***

Dans un **Guide pratique de la sécurité** publié en décembre 2009, le **Haut fonctionnaire de défense et de sécurité** (HFDS) du ministère de l'économie, qui "*conseille et assiste les ministres pour toutes les questions relatives aux mesures de défense et de sécurité, tout particulièrement dans le domaine de la défense économique*", a une solution toute trouvée : "***le PC portable doit être évité dans la mesure du possible***".

> ***Privilégiez les solutions suivantes :***
>
> ***- Emportez vos fichiers sur un, voire deux, à titre de sauvegarde, support amovible que vous gardez avec vous (les médias de sauvegarde sont régulièrement mis à jour et rangés dans deux bagages distincts).***
> ***- Préférez la mise à disposition d'un PC de l'entreprise sur place, dans un environnement de confiance. Dans ce cas, emportez vos fichiers sur unsupport amovible, si possible chiffré en fonction de la législation locale relative aux transmissions chiffrées et gardez ce support en permanence avec vous.***
>
> ***Si le PC portable est indispensable :***
>
> ***- Contrôle d'accès au démarrage avec un mot de passe fort et/ou biométrie.***
> ***- Données dans la partition chiffrée du disque dur ou sur un support amovible chiffré et sous surveillance permanente.***
> ***- Banalisez le transport de l'ordinateur portable (pas de sacoche portant la marque du fabriquant…).***
> ***- Ne relâchez jamais la surveillance de votre PC (il voyage en cabine avec vous).***
> ***- Rappelez-vous que toutes les liaisons hertziennes (wifi, bluetooth, carte 3G…) à partir d'un PC, PDA ou téléphone portable peuvent être interceptées.***

…à défaut, restez vierges



Sous-titré "*Partir en mission avec son téléphone mobile, son assistant personnel ou son ordinateur portable*", le **Passeport de conseils aux voyageurs**, co-signé Patrick Pailloux, directeur général de l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**, rattachée au Secrétaire général de la défense nationale), et Régis Poincelet, vice président du Club des directeurs de sécurité des entreprises (**CDSE**), rappelle lui aussi que "*les cybercafés, les hôtels, les lieux publics et parfois même les bureaux de passage n'offrent pas de garantie de confidentialité. Dans de nombreux pays étrangers, les centres d'affaires et les réseaux téléphoniques sont surveillés. Dans certains, les chambres d'hôtel peuvent être fouillées*".

Le guide commence par rappeler qu'au premier chef, les appareils "*ne doivent contenir aucune information autre que celles dont vous avez besoin pour la mission*" et que doivent en particulier être proscrites les "*photos, vidéos, ou œuvres numériques qui pourraient vous placer en difficulté vis-à-vis de la législation ou des mœurs du pays visité*".

Règle n°1 : ne jamais partir en voyage avec son ordinateur personnel, ni de travail, mais de ne voyager qu'avec un disque dur vierge de toute donnée.
Règle n°2 : prenez connaissance de la législation locale .
Règle n°3 : sauvegardez les données que vous emportez , "vous récupérerez ainsi vos informations à votre retour en cas de perte, de vol ou de saisie de vos équipements".
Règle n°4 : évitez de partir avec vos données sensibles . "Privilégiez, si possible, la récupération de fichiers chiffrés sur votre lieu de mission en accédant :
- au réseau de votre organisme avec une liaison sécurisée, par exemple avec un client VPN mis en place par votre service informatique.
- sinon à une boîte de messagerie en ligne spécialement créée et dédiée au transfert de données chiffrées (via https) et en supprimant les informations de cette boite après lecture".
Règle n°5 : emportez un filtre de protection écran pour votre ordinateur si vous comptez profiter des trajets pour travailler vos dossiers, afin d'éviter que des curieux lisent vos documents par-dessus votre épaule.
Règle n°6 : mettez un signe distinctif sur vos appareils (comme une pastille de couleur), "cela vous permet de pouvoir surveiller votre matériel et de vous assurer qu'il n'y a pas eu d'échange, notamment

pendant le transport. Pensez à mettre un signe également sur la housse".

A noter, en complément de la règle n°4, un **petit truc**, inspiré de la technique bien connue de la **boîte aux lettres morte** et qui aurait été utilisé par des terroristes pour échapper à la surveillance étatique : p**artager une boîte aux lettres électroniques, en n'y écrivant qu'en mode brouillon : les emails ne sont dès lors pas échangés, ils ne circulent pas sur les réseaux**, et ne peuvent donc être consultés que par ceux qui se sont connectés (de façon sécurisée, via https) à la boîte aux lettres en question.

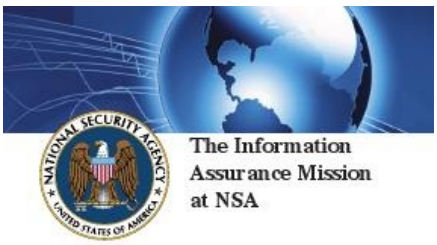
Chiffrez l'intégralité de vos données

D'un point de vue plus technique, le passeport recommande de "***configurer les appareils de manière défensive***", et donc d'installer sur vos appareils numériques de quoi "*résister aux attaques informatiques et éviter le vol de données*" :

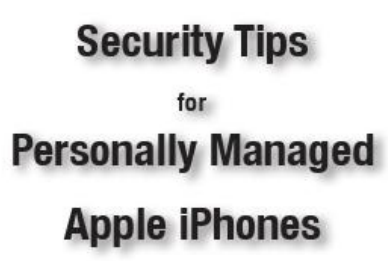
- Désactivez les liaisons inutilisées (Bluetooth, infrarouge, wifi, …) et les services inutiles ;
- Paramétrez le pare-feu et le navigateur de manière restrictive;
- Utilisez un compte sans droits administrateur;
- Mettez à jour les logiciels (système d'exploitation, navigateur, anti-virus, pare-feu personnel, etc…);
- Désactivez l'exécution automatique des supports amovibles (CDROM, Clés USB);
- Désactivez les services de partage de fichiers et d'imprimantes.

Afin de garantir la confidentialité des données, il convient également d'**installer "*un logiciel qui assure le chiffrement de l'environnement complet de travail (disque dur, fichiers temporaires, fichier d'échange, mémoire)"*** pour ce qui est des ordinateurs portables, d'"*un logiciel assurant le chiffrement de l'intégralité du répertoire de contacts, de l'agenda et des messages*" pour les PDA et les Smartphone ("*à défaut, activez la protection d'accès par code PIN*").

On peut également se reporter au **manuel** de sécurisation des iPhone publié par la National Security Agency américaine (chargée d'espionner les télécommunications du monde entier, mais également de sécuriser celles des Américains), publié en décembre 2009, et dont la plupart des conseils peuvent également s'appliquer aux autres modèles de téléphones portables.



La NSA y rappelle au premier chef de ne jamais



se séparer physiquement de son mobile, dès lors qu'il existe des logiciels et outils qui, une fois installés sur les appareils, permettent de les **écouter** à distance.

De même, et à l'instar des bonnes pratiques recommandées pour ce qui est des ordinateurs, **il est vivement conseillé de protéger l'accès aux données par un mot de passe** (la plupart des téléphones permettent de paramétrer un écran de veille qui ne peut être désactivé que par un mot de passe), voire de le configurer de sorte que le téléphone efface toutes les données après X tentatives infructueuses d'y accéder.

Dans la mesure du possible, évitez d'utiliser le Wifi (sauf s'il est vraiment sécurisé, de préférence en **WPA2**), et désactivez bien évidemment le BlueTooth, ainsi que la géolocalisation.

Le n°24 de la revue **ActuSécu**, paru en janvier 2010, revient en détail sur les problèmes de sécurité des iPhone. Tout comme la NSA, **elle déconseille fortement de "*jailbreaker*" son téléphone.**

Cette opération, consistant à passer outre les restrictions imposées par Apple afin d'y installer un autre système d'exploitation, installe en effet par défaut un "***serveur***" sur le téléphone, serveur qui, ouvert, offre la possibilité à des individus mal intentionnés de s'y connecter, et d'y récupérer l'intégralité des données…

Ceux qui, malgré tout, voudraient jailbreaker leur iPhone prendront le soin de modifier les mots de passe des comptes `root` et `mobile`. Par défaut, ces deux comptes ont le même mot de passe : `alpine`…

Bon voyage

Une fois ces règles bien comprises, et vos appareils et systèmes de communication paramètres de sorte d'être correctement sécurisées, "*vous disposez maintenant des bons bagages pour partir en toute sécurité…*", ou presque, comme le rappellent les auteurs du rapport, au chapitre "***Pendant la mission***" :

> ***1) Gardez vos appareils, support et fichiers avec vous !***
> ***Prenez-les en cabine lors de votre voyage. Ne les laissez pas dans un bureau ou dans la chambre d'hôtel (même dans un coffre).***
> ***2) Si vous êtes contraint de vous séparer de votre téléphone portable ou de votre PDA, retirez et conservez avec vous la carte SIM ainsi que la batterie.***
> ***3) Utilisez un logiciel de chiffrement pendant le voyage.***
> ***Ne communiquez pas d'information confidentielle en clair sur votre téléphone mobile ou tout autre moyen de transmission de la voix.***
> ***4) Pensez à effacer l'historique de vos appels et de vos navigations (données en mémoire cache, cookies, mot de passe d'accès aux sites web et fichiers temporaires).***
> ***5) En cas d'inspection ou de saisie par les autorités, informez votre organisme.***
> ***Fournissez les mots de passe et clés de chiffrement, si vous y êtes contraint par les autorités locales.***
> ***6) En cas de perte ou de vol d'un équipement ou d'informations, informez immédiatement votre organisme et demandez conseil au consulat avant toute démarche auprès des autorités locales.***
> ***7) N'utilisez pas les équipements qui vous sont offerts avant de les avoir fait vérifier par votre service de sécurité. Ils peuvent contenir des logiciels malveillants.***
> ***8) Evitez de connecter vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance.***
> ***Attention aux échanges de documents (par exemple : par clé USB lors de présentations commerciales ou lors de colloques). Emportez une clé destinée à ces échanges et effacez les fichiers, de préférence avec un logiciel d'effacement sécurisé.***

La sécurité est un process, pas un produit

Dans un autre accès de clairvoyance, Bruce Schneier avait également déclaré que "*Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie*".

Dit autrement, la sécurité est un processus, pas un produit, et rien n'est pire qu'un faux sentiment de sécurité engendré par une accumulation de "*trucs*" ou parce qu'on a acheté tel ou tel "***produit***" ou logiciel de sécurité.

Les auteurs du rapport rappellent ainsi qu'"***avant votre retour de mission*** ", un certain nombre d'autres mesures de protection s'avèrent, sinon indispensables, tout du moins fortement conseillées :

> ***1) Transférez vos données***
>
> ***- sur le réseau de votre organisme à l'aide de votre connexion sécurisée ;***
> ***- sinon sur une boite de messagerie en ligne dédiée à recevoir vos fichiers chiffrés (qui seront supprimés dès votre retour). Puis effacez les ensuite de votre machine, si possible de façon sécurisée, avec un logiciel prévu à cet effet.***
>
> ***2) Effacez votre historique de vos appels et de vos navigations***
>
> ***Après la mission, tout particulièrement si votre équipement a échappé à votre surveillance :***
>
> ***1) Changez les mots de passe que vous avez utilisés pendant votre voyage.***
> ***2) Analysez ou faites analyser vos équipements .***
> ***"Ne connectez pas les appareils à votre réseau avant d'avoir fait au minimum un test anti-virus et anti-espiogiciels".***

Ayez une bonne hygiène… du mot de passe

De façon plus générale, il est de toute façon recommandé d'avoir une bonne hygiène du mot de passe, et donc de ne jamais les écrire sur des bouts de papier, de toujours mêler lettres minuscules, majuscules, chiffres et caractères spéciaux, d'en changer régulièrement, et de **ne surtout pas utiliser un seul et même mot de passe pour les comptes les plus importants…**

L'une des techniques préférées des pirates informatiques, et des espions, est d'installer un "***cheval de Troie***" sur l'ordinateur de leurs victimes, afin d'en prendre le contrôle ou, via un "***keylogger***" (enregistreur de touches de clavier) de capturer leurs mots de passe, et donc d'être maître de leurs ordinateurs.

Une technique fort utilisée en matière d'espionnage industriel lorsque la personne à espionner n'a pas d'ordinateur, et que c'est l'espion qui le lui fournit… et que le gouvernement français s'apprête, lui aussi, à autoriser. La Loppsi **prévoit** en effet de donner la possibilité aux forces de l'ordre d'installer de tels mouchards ou logiciels espions sur les ordinateurs des personnes suspectées de crimes en "*bande organisée*", notion fourre-tout melant terrorisme, vols, trafic de drogue, proxénétisme mais également l'aide à l'immigration clandestine, il n'est pas inutile de savoir comment saisir un mot de passe sans risque de le voir intercepté.

A la manière des antivirus, il existe des **anti-keyloggers**, mais ils sont payants, et ne détectent généralement que les keyloggers connus existants sur le marché. **Deux techniques, relativement simples, permettent a priori de se prémunir contre ce genre**

de mouchards : la première, et plus connue, consiste à **utiliser le clavier virtuel de son ordinateur** (certaines banques en ligne en propose aussi), et donc de, non pas taper le mot de passe sur le clavier, mais de le cliquer, avec la souris.

L'autre technique, **exposée** par le blogueur Korben, consiste à **taper un grand nombre de caractères, de manière aléatoire, en parallèle à la saisie du mot de passe**. Ainsi, et au lieu d'entrer, par exemple, m0T2p4$s3, l'utilisateur averti saisira dans le formulaire m0 puis, à côté, dans le vide, une suite de caractère aléatoire, puis T2, etc. De la sorte, ce qui aura été capté par le keylogger ou le cheval de Troie se présentera sous la forme : m0ezrf45T2sdfv84p4zrtg54$s3zerg48, rendant bien plus difficile la fuite du mot de passe.

La sécurité, ça se mérite, et ça s'apprend

Une chose est d'apprendre à sécuriser son mot de passe, et de chiffrer l'intégralité de son disque dur, et donc les données qui y sont inscrites, une autre est d'éviter qu'elles ne fuitent. Les auteurs du passeport conseillent ainsi d'installer "*un logiciel d'* ***effacement sécurisé*** *des fichiers afin de pouvoir éventuellement supprimer toutes les données sensibles lors du déplacement*", mais également de "*configurer le serveur et le client de messagerie pour que les transferts de messages soient chiffrés par les protocoles SSL et TLS*".

Tout ceci vous paraît cryptique ? Allons… **De même que c'est en pédalant que l'on apprend à faire du vélo, c'est en contre-espionnant que l'on apprend à se protéger.** Avec un peu d'entraînement, vous apprendrez à maîtriser les techniques et outils qui correspondent à vos besoins. Avec un peu de pratique, elles deviendront des réflexes. La sécurité, ça se mérite, et ça s'apprend.

Pour certains, la paranoïa est un métier, en tout cas une tournure d'esprit les invitant, en constance, à la prudence. Mais pour la majeure partie des gens, la question est moins de se protéger, en tout temps, que de savoir comment protéger telles ou telles données, de savoir comment ne pas laisser de traces, ou comment les effacer.

L'important est de bien mesurer les risques encourus, les menaces auxquels vous avez à faire face, et d'y répondre par la ou les techniques appropriées, au moment opportun. Comme je le rappelais par ailleurs dans "**Comment contourner la cybersurveillance**", aucune solution n'est fiable à 100% et rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. Il convient d'autre part de ne jamais oublier qu'en matière informatique en générale, et sur l'internet en particulier, l'anonymat n'existe pas. Il arrive fatalement un moment où l'on se trahit, où l'on commet une erreur, ou, plus simplement, où l'on tombe sur quelqu'un de plus fort que soi.

La sécurité informatique est un métier, elle ne s'improvise pas. Par contre, elle s'apprend. Pour en savoir plus sur les outils et technologies à utiliser, voici quelques liens, sites web et ressources susceptibles, a priori, de répondre à toutes vos questions :

. "**Comment contourner la cybersurveillance**", l'article que j'avais rédigé pour le CNRS, et basé sur un article rédigé par l'ancien directeur des communications électroniques de la Défense britannique et de l'OTAN,

. "**Security in a box**", mode d'emploi (en français) bien plus pratique et détaillé, réalisé par deux ONG de défense des droits humains à l'ère de l'information,

. le **Wiki de l'internet libre** de **Korben.info**, qui regorge d'informations pratiques sur la sécurité informatique,

. le **Guide d'autodéfense numérique** qui explique, pas à pas, comment configurer son ordinateur (hors connexions internet) de façon sécurisée en fonction des risques encourus,

. les **10 commandements de la sécurité informatique**, sur securite-informatique.gouv.fr, et ses **modules d'autoformation**, notamment ceux consacrés aux **Principes essentiels de la sécurité informatique**, à la **Sécurité du poste de travail** et aux **mots de passe**.

. **Ordinateur & Sécurité Internet, Vie Privée, Anonymat et cætera**, qui fut un temps considéré comme une menace par le FBI parce qu'expliquant aux internautes comment apprendre à rester anonyme.

. **Guide pratique du chef d'entreprise face aux risques numériques** (.pdf) rendu public à l'occasion du **Forum International sur la Cybercriminalité** et rédigé par des gendarmes, policiers, juristes et professionnels de la sécurité informatique,

. les **12 conseils pour protéger votre vie privée en ligne** de l'Electronic Frontier Foundation et son **manuel d'auto-défense** numérique (en anglais), rédigé pour aider les internautes confrontés à des régimes autoritaires, ainsi que, et toujours en anglais :

. **Hints and Tips for Whistleblowers**

. **BlogSafer: Speak Freely and Stay Free**

. **Digital Security and Privacy for Human Rights Defenders**

—

Retrouvez les deux autres articles de ce **second volet** de notre série sur le Contre-espionnage informatique : **Nokia, histoire d'un fail corporate** et **Comment contourner la cybersurveillance** ?

Retrouvez également le **premier** et **dernier** volet de cette série sur le contre-espionnage.

GUILLAUME
le 25 mai 2010 - 19:14 • SIGNALER UN ABUS - PERMALINK

Citer Bruce Shneier comme expert en sécurité et conseiller de ne pas écrire ses mots de passe, c'est assez antinomique, je trouve…

http://www.schneier.com/blog/archives/2005/06/write_down_your.html

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

HUXLEY
le 8 juin 2010 - 0:51 • SIGNALER UN ABUS - PERMALINK

Non mais quel tissus de conneries !
- "Quand vous voyagez, n'emmenez aucun fichier avec vous, seulement un disque dur vierge, et téléchargez le tout sur place": ce type n'a manifestement jamais été amené à voyager pour des raisons professionnelles…
- "Faites-vous prêter un PC sécurisé une fois sur place": ben voyons, tous mes clients, partenaires et même prospects ont une batterie de PC à disposition à prêter à un glandu comme moi; d'ailleurs leur IT gère non seulement le parc de PC sécurisés de la société, mais aussi les PC pour les visiteurs. Et puis c'est vachement pratique de bosser sur une machine dont l'environnement est radicalement différent de celui installé sur son propre PC pro encastré dans un pilier de béton armé au troisième sous-sol
- Utilisez des mots de passe mélangeant majuscules/minuscules/chiffres/ronds dans l'eau et variez les mots de passes parmi vos différents comptes: j'ai au boulot une dizaine de comptes différents, avec en plus des contraintes de mots passe différentes voire incompatibles… Comment croyez-vous que je (ingénieur en informatique en théorie) gère cela ? Et la secrétaire qui ne comprend rien au PC ?
- Et la cerise sur le gâteau: exploiter les conseils de la NSA… Quelque chose me dit que le principal organisme chargé de la surveillance aux US a intérêt à ce que vous utilisiez des méthodes qu'il sait pouvoir contourner, non ?

C'est beau la théorie… la pratique est souvent plus hardue…

VOUS AIMEZ 2 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

SKHAEN
le 30 juin 2010 - 0:00 • SIGNALER UN ABUS - PERMALINK

Article très intéressant, juste un léger point à rajouter :

"Dans la mesure du possible, évitez d'utiliser le Wifi (sauf s'il est vraiment sécurisé, de préférence en WPA)"

C'est pas totalement vrai, c'est WPA+AES, le WPA+TKIP étant cassable en quelques minutes depuis maintenant quelques années …

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JOHNATHAN REYNOLDSON
le 29 août 2010 - 2:35 • SIGNALER UN ABUS - PERMALINK

hi all, i'm really bored on the internet so you all should email moi if ya are also,

strike up a convo :). or possibly facebook, my name on there is brittany kowalski

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

CORY TROWEL
le 30 août 2010 - 5:41 • SIGNALER UN ABUS - PERMALINK

hey all, i'm really bored on the net so you all should email me if you are also, strike up a convo :). or possibly myspace, my name on there is johnny miller

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ORDINATEUR DE BUREAU
le 5 septembre 2010 - 1:50 • SIGNALER UN ABUS - PERMALINK

The Zune concentrates on being a Portable Media Player. Not a web browser. Not a game machine. Maybe in the future it'll do even better in those areas, but for now it's a fantastic way to organize and listen to your music and videos, and is without peer in that regard. The iPod's strengths are its web browsing and apps. If those sound more compelling, perhaps it is your best choice.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MOREL
le 18 février 2011 - 4:55 • SIGNALER UN ABUS - PERMALINK

J'ai tout essayé pour me débarrasser d'un truc qui s'appel " double click ", mais en vain, j'ai fouillé sur les forums j'ai essayé plusieurs astuces conseillées, rien à faire cela est récurrent.(je me suis aussi informé sur ce fameux " double click ".)(no comment …)
Donc qui pourrai me dire comment m'en débarrasser.
Merci,

Jean-Louis

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LIBRE FAN
le 15 mai 2011 - 12:45 • SIGNALER UN ABUS - PERMALINK

Très bonne initiative que cette information détaillée. Vous pouvez rajouter Facebook et tous les services Google: précautions avant et pendant le voyage.

Il faudrait cependant commencer par donner l'exemple sur OWNI en ne mettant pas de cartes Google Maps (voir OWNIshiste).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

WALLACE TUKUAFA
le 24 juillet 2011 - 19:19 • SIGNALER UN ABUS - PERMALINK

hi, it's very nice blog , thank you to the admin

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LASER EYE SURGERY
le 19 novembre 2011 - 7:38 • SIGNALER UN ABUS - PERMALINK

Why didnt I think about this? I hear exactly what youre saying and Im so happy

that I came across your blog. You really know what youre talking about, and you made me feel like I should learn more about this. Thanks for this; Im officially a huge fan of your blog

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DAHOUMANE HAMZA
le 28 janvier 2012 - 11:30 • SIGNALER UN ABUS - PERMALINK

si la vache avait une queue ce serait un boeuf.est il vrai?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DAHOUMANE HAMZA
le 28 janvier 2012 - 11:36 • SIGNALER UN ABUS - PERMALINK

que fait l'otan?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MARCEL
le 23 mars 2012 - 10:19 • SIGNALER UN ABUS - PERMALINK

Article passionnant. Merci.
Dans la dernière phrase, les deux "liens vers le premier et le dernier volet de cette série" ne fonctionnent pas (on abouti à une page vide).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MG
le 7 septembre 2012 - 12:08 • SIGNALER UN ABUS - PERMALINK

Je tombe là dessus avec retard. Attention au truc de Korben (rubrique antikeylogger) si vous êtes dans un pays sensible: il suffit de comparer trois ou quatre saisies pour éliminer le "bruit" et retomber sur le mot de passe, qui reste invariant d'une saisie à l'autre, car cela isolera les frappes aléatoires (paradoxalement, il faudrait ne pas taper de suite aléatoire pour compliquer les choses, mais ça ne les compliquera ni beaucoup ni longtemps).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ZEIGWAH
le 7 septembre 2012 - 20:54 • SIGNALER UN ABUS - PERMALINK

Bonjour !

Je tiens juste à signaler un liens mort dans votre article (qui est très intéressant en passant) situé vers la fin du texte.

C'est le liens concernant Security in a box :
"Security in a box, mode d'emploi (en français) bien plus pratique et détaillé, réalisé par deux ONG de défense des droits humains à l'ère de l'information"

L'URL correcte serait d'après une rapide recherche : https://securityinabox.org/fr

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

AES
le 10 septembre 2012 - 11:25 • SIGNALER UN ABUS - PERMALINK

Comment sécurisé un computer portable, lorsqu'il existe des softs pouvant casser n'importes quelles clés de protection. Il faut dabord, interdire l'accès à l'ordinateur par les ports USB et carte mémoire, ensuite, un bon programme de cryptage des fichiers genre PGP256bit est vivement conseiller, enfin. acheter un vieux disk dur, lui injecteé du 12v ou 24v, faisant croire à un retour éléctrique durant un orage et retirer le disk dur principal du PC portable. N'importe qui peu faire cela, meme les gamins. Ensuite voyager en racontant que vous cherchez à le faire réparer pour moindre coût. Aujourd'hui, il est des micro sd card mémoire de 64Gb, voire peut-être 128Gb (je n'en suis pas sur), mais ce genre de carte, se glisse facilement dans un vieux téléphone céllulaire, un briquet, un porte-clé, un ipod musical, bref, n'importe quel objet que nous pouvons trouver sur le marché mondial, ou sur Ebay.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

LAURENT OUTANG
le 29 septembre 2012 - 11:47 • SIGNALER UN ABUS - PERMALINK

TOR + TAILS + GPG + TrueCrypt + Pidgin OTR + TorServ + Untraceable encrypted phones with everchanging IEM….

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

33 pings

Les tweets qui mentionnent Petit manuel de contre-espionnage informatique » Article » owni.fr, digital journalism -- Topsy.com le 24 mai 2010 - 9:22

[...] Ce billet était mentionné sur Twitter par Mehdi Lamloum et Owni, Haythem El Mekki. Haythem El Mekki a dit: RT @MehdiLamloum RT @0wn1: [#owni] Petit manuel de contre-espionnage informatique http://goo.gl/fb/omQdy [...]

telecomsenegal.com » Eric Filliol: "l'Etat doit s'appuyer sur les hackers" le 25 mai 2010 - 13:20

[...] les hackers, plutôt que de continuer à les diaboliser. Une interview à lire en complément du Petit manuel de contre-espionnage informatique que je publie en parallèle sur [...]

Leur faire peur « C.C.E. le 27 mai 2010 - 21:14

[...] trouve tant de choses sur Internet . Pensez quand même à passer par la lecture d'un petit manuel du contre-espionnage ou plus simplement par un proxy externe, voir interne comme Tor ,avant d'aller fourrer [...]

Eric Filliol : "L'Etat doit s'appuyer sur les hackers" - Affairer.com – Le site de l'affairage le 31 mai 2010 - 11:41

[...] les hackers, plutôt que de continuer à les diaboliser. Une interview à lire en complément du Petit manuel de contre-espionnage informatique que je publie en parallèle sur Owni.fr. Source This entry was posted on Lundi, mai 31st, [...]

Gola profonda: come assicurare la copertura delle fonti nell' era della sorveglianza totale | LSDI le 4 juin 2010 - 22:27

[...] aver pubblicato nei giorni scorsi su Owni.fr un piccolo manuale di controspionaggio informatico, Jean Marc Manach spiega come fare per contattare qualcuno, facilmente e in maniera supersicura, in [...]

links for 2010-06-01 « Les Giraultises blogguent le 9 juin 2010 - 6:05

[...] Petit manuel de contre-espionnage informatique » Article » owni.fr, digital journalism Autrefois réservés aux seuls services secrets, les outils et technologies de surveillance, GPS, téléphones et logiciels espions, se “démocratisent” au point que, suite à un reportage de M6, Petits espionnages en famille, montrant comment de plus en plus de gens espionneraient les téléphones portables et ordinateurs de leur futurs (ou ex-) femmes (ou maris), enfants, nounous, Le Parisien/Aujourd’hui en France faisait sa “une”, début 2010, sur la question (Votre portable devient espion), tout en expliquant qu’espionner les téléphones portables était devenu “un jeu d’enfant” (à toutes fins utiles, en France, leur commercialisation, mais également leur simple détention, n’en est pas moins punie d’un an de prison et de 45 000 euros d’amende). [...] Le fait est que, et aussi paradoxal que cela puisse être, la CNIL explique bien, par exemple, comment nous sommes tracés sur le Net… mais sans jamais nous expliquer comment s’en protéger. (tags: securite information conseil hacking liste voyage entreprise espionnage surveillance) [...]

JEAN-MARC MANACH: « LE PROBLÈME C’EST LA SURVEILLANCE, PAS LA TRANSPARENCE « Libertes & Internets le 2 juillet 2010 - 9:09

[...] à s’y protéger. Voir aussi, à ce titre, Comment contourner la cybersurveillance ?, mon Petit manuel de contre-espionnage informatique, ainsi que Gorge profonde, le mode d’emploi, qui explique comment garantir la confidentialité de [...]

Verbose : Anonymat sur Internet « GNU-It le 7 juillet 2010 - 13:44

[...] finir, un Petit manuel de contre-espionnage informatique. A bientôt sur GNU-It. =) Mots-clefs :anonymat, astuces, Browser, gouvernement, guides, [...]

Sécurité informatique, les fondamentaux ! — Par Solstice et Agronome | Centre d'Etude et d'Enseignement des Techniques de Survie le 3 février 2011 - 11:08

[...] seul lien à pouvoir vous proposer pour prolonger cet article, nous choisirions celui-ci : http://owni.fr/2010/05/24/petit-manuel-de-contre-espionnage-informatique/ . Si son contenu est en lui-même intéressant, les liens proposés en fin d’article sont [...]

[Criminalisation du militantisme] (et du journalisme!) Petit manuel de contre-espionnage informatique | Club de l'Europe le 9 mars 2011 - 15:33

[...] Petit manuel de contre-espionnage informatique » Article » OWNI, Digital Journalism. [...]

Petit manuel de contre-espionnage informatique « Cybercriminalité, sécurité et ordre public le 17 avril 2011 - 6:51

[...] Tout savoir [...]

L’enfer, c’est les « internautres » | BUG BROTHER le 1 juin 2011 - 17:30

[...] des "internAutres" : Gorge profonde : le mode d'emploi Journalistes : protégez vos sources ! Petit manuel de contre-espionnage informatique Comment contourner la cybersurveillance ? Voir aussi ce très complet manuel en français (et en [...]

En vrac #67 « wOueb by Romain DECKER / Another IT Guy Blog le 23 septembre 2011 - 14:12

[...] Les menaces ne viennent pas toujours d’où on pense, c’est pourquoi quelques bons conseils sont toujours bon à prendre : petit manuel de contre-espionnage informatique.

[...]

Petit manuel de contre-espionnage informatique | PROTEGOR, blog de sécurité personnelle, self-défense & survie urbaine le 8 octobre 2011 - 17:42

[...] Petit manuel de contre-espionnage informatique est un article retrouvé dans mes « logs » de sujets à partager et que j'avais un peu oublié, oops… du coup ce n'est pas « tout frais », mais certains seront sûrement de le découvrir ! [...]

Internet massivement surveillé « annie bannie's Weblog le 14 décembre 2011 - 15:16

[...] et donc de sécurité informatique, voir notamment « Gorge profonde: le mode d'emploi » et « Petit manuel de contre-espionnage informatique [...]

Le Petit Monde Cozillon » Des chevaux de Troie dans nos démocraties le 11 janvier 2012 - 19:42

[...] Afin de répondre aux risques d'espionnage informatique, ou de pertes de données confidentielles, les autorités elle-mêmes encouragent les entreprises à apprendre à leurs salariés comment s'initier à la sécurité informatique, et sécuriser leurs communications (voir, à ce titre, mon Petit manuel de contre-espionnage informatique). [...]

Vie privée : le guide pour rester anonyme sur Internet | Rue 89 | Actualités des Journaux le 2 février 2012 - 13:51

[...] du béton frais : on laisse des traces (presque) indélébiles partout. C'est aussi ce que dit Bruce Schneier, expert en sécurité informatique : « Si vous pensez que la technologie peut [...]

PETIT GUIDE POUR RESTER ANONYME SUR INTERNET (mais vous n'êtes pas en sécurité pour autant) « Libertes & Internets le 2 février 2012 - 17:12

[...] du béton frais : on laisse des traces (presque) indélébiles partout. C'est aussi ce que dit Bruce Schneier, expert en sécurité informatique : « Si vous pensez que la technologie peut [...]

De l'Internet | Pearltrees le 7 mars 2012 - 12:26

[...] – Données dans la partition chiffrée du disque dur ou sur un support amovible chiffré et sous surveillance permanente. Petit manuel de contre-espionnage informatique » OWNI, News, Augmented [...]

Cybercriminalité | Pearltrees le 7 mars 2012 - 21:28

[...] – Données dans la partition chiffrée du disque dur ou sur un support amovible chiffré et sous surveillance permanente. – Banalisez le transport de l'ordinateur portable (pas de sacoche portant la marque du fabriquant…). – Contrôle d'accès au démarrage avec un mot de passe fort et/ou biométrie. Petit manuel de contre-espionnage informatique » OWNI, News, Augmented [...]

Barbouzeries au Pays de « Candy » | BUG BROTHER le 16 mars 2012 - 15:05

[...] email valide (mais anonyme). PLus d'explications : « Gorge profonde: le mode d'emploi » et « Petit manuel de contre-espionnage informatique ». Voir aussi [...]

OUTILS | Pearltrees le 22 mars 2012 - 15:49

[...] GPS, téléphones portables, logiciels espions: les outils de la surveillance se démocratisent. Conseils utiles pour s'en protéger. Autrefois réservés aux seuls services secrets, les outils et technologies de surveillance, GPS, téléphones et logiciels espions, se " démocratisent " au point que, suite à un reportage de M6, Petits espionnages en famille , montrant comment de plus en plus de gens espionneraient les téléphones portables et ordinateurs de leur futurs (ou ex-) femmes (ou maris), enfants, nounous, Le Parisien/Aujourd'hui en France faisait sa "une", début 2010, sur la question (Votre portable devient espion), tout en expliquant qu'espionner les téléphones portables était devenu " un jeu d'enfant " (à toutes fins utiles, en France, leur commercialisation, mais également leur simple détention, n'en est pas moins punie d'un an de prison et de 45 000 euros d'amende). Petit manuel de contre-espionnage informatique » OWNI, News, Augmented [...]

Petit manuel de contre-espionnage informatique « lyness, stagiaire CATIC le 7 septembre 2012 - 11:32

[...] en savoir plus:http://owni.fr/2010/05/24/petit-manuel-de-contre-espionnage-informatique/ Share this:TwitterFacebookJ'aime ceci:J'aimeSoyez le premier à aimer ceci. Classé dans [...]

Facebook et le « paradoxe de la vie privée » | BUG BROTHER le 25 septembre 2012 - 7:46

[...] Accessoirement -si j'ose dire-, les gens n'ont pas attendu ce "bug" pour espionner leurs conjoints, enfants, parents, collègues, employés, patrons, colocataires, etc. : l'espionnage de la correspondance privée, autrefois réservé aux seuls services de renseignement et barbouzes, est aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook et le « paradoxe de la vie privée » | Résistance Inventerre le 26 septembre 2012 - 0:07

[...] Accessoirement – si j'ose dire –, les gens n'ont pas attendu ce "bug" pour espionner leurs conjoints, enfants, parents, collègues, employés, patrons, colocataires, etc. : l'espionnage de la correspondance privée, autrefois réservé aux seuls services de renseignement et barbouzes, est aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook et le « paradoxe de la vie privée » | News & Buzz le 26 septembre 2012 - 12:10

[...] Accessoirement – si j'ose dire –, les gens n'ont pas attendu ce « bug » pour espionner leurs conjoints, enfants, parents, collègues, employés, patrons, colocataires, etc. : l'espionnage de la correspondance privée, autrefois réservé aux seuls services de renseignement et barbouzes, est aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook et le « paradoxe de la vie privée » ! « besocialweb le 30 septembre 2012 - 14:46

[...] Accessoirement – si j'ose dire –, les gens n'ont pas attendu ce "bug" pour espionner leurs conjoints, enfants, parents, collègues, employés, patrons, colocataires, etc. : l'espionnage de la correspondance privée, autrefois réservé aux seuls services de renseignement et barbouzes, est aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Revue de presse du lundi | Internet | NRE's Blog le 2 octobre 2012 - 16:34

[...] Petit manuel du contre-espionnage informatique. [...]

Facebook sait si vous êtes gay, Google que vous êtes enceinte. Et ta soeur ? l BUG BROTHER le 3 octobre 2012 - 9:06

[...] En matière de protection de la vie privée, le problème se situe (aussi) entre la chaise et le clavier… d'autant plus que les outils d'espionnage informatique, qui étaient autrefois l'apanage des seuls services de renseignement, sont aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook sait si vous êtes gay, Google que vous êtes enceinte. Et ta soeur ? « Breves de La Vigi le 3 octobre 2012 - 13:28

[...] En matière de protection de la vie privée, le problème se situe (aussi) entre la chaise et le clavier… d'autant plus que les outils d'espionnage informatique, qui étaient autrefois l'apanage des seuls services de renseignement, sont aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Monde : Facebook sait si vous êtes gay, Google que vous êtes enceinte. Et ta soeur ? « Quartier Didot – Porte de Vanves le 9 octobre 2012 - 15:27

[...] de renseignement, sont aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook et le « paradoxe de la vie privée » l blogjolienetelise le 25 octobre 2012 - 18:01

[...] Accessoirement – si j'ose dire –, les gens n'ont pas attendu ce « bug » pour espionner leurs conjoints, enfants, parents, collègues, employés, patrons, colocataires, etc. : l'espionnage de la correspondance privée, autrefois réservé aux seuls services de renseignement et barbouzes, est aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). [...]

Facebook sait si vous êtes gay, Google que vous êtes enceinte. Et ta soeur ? « projetfrancais1 le 29 octobre 2012 - 21:10

[...] renseignement, sont aujourd'hui à la portée de n'importe qui, ou presque (voir mon petit manuel de contre-espionnage informatique). Share this:TwitterFacebookJ'aime ceci:J'aimeSoyez le premier à aimer [...]