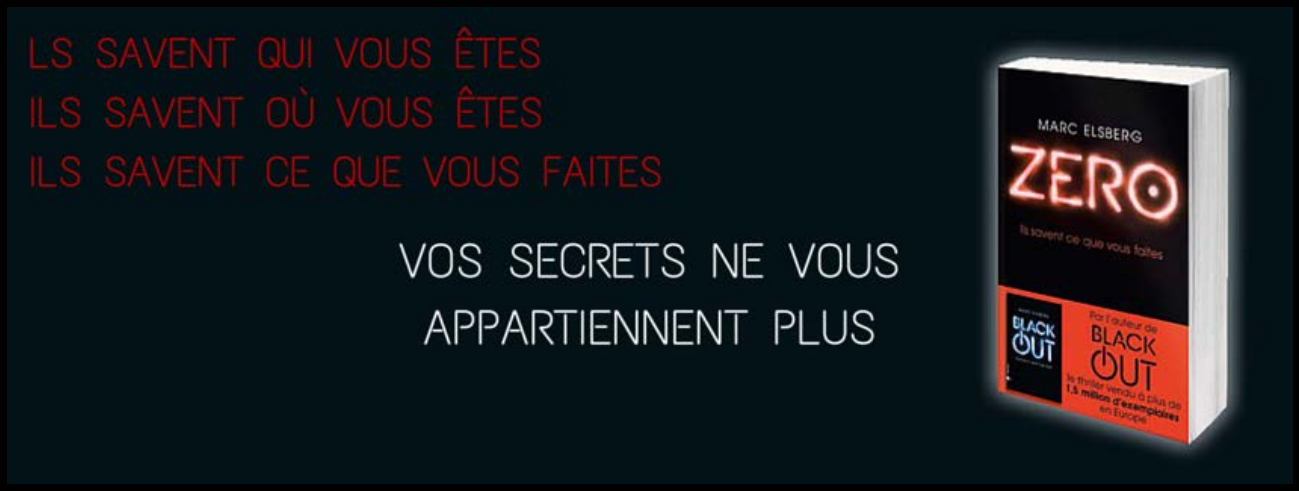


Surfer sur le web de manière anonyme…

Quelles traces laissez-vous derrière vous sur Internet ? Vous trouverez quelques informations ici. Vous en apprendrez davantage sur le sujet par exemple sur computerbetrug.de ou dans nos liens.

1ère trace : l'adresse IP

Chaque ordinateur a sa propre adresse IP individuelle. C'est, pour ainsi dire, votre adresse postale sur Internet, à laquelle toutes les informations doivent se rendre : les résultats d'une recherche Google, les appels d'un site Internet, les téléchargements de fichiers etc. Votre adresse IP est envoyée de manière invisible à l'ordinateur avec lequel votre PC est en train de communiquer. Ainsi, ce dernier sait où il doit envoyer ses données afin que vous les receviez également. Inversement, il est par exemple « facile » pour les instances enquêtrices de remonter votre adresse IP, donc votre trace, jusqu'à chez vous.

2ème trace : les données de connexion

Lorsque vous vous connectez à Internet, votre prestataire de service stocke vos données de connexion, parmi lesquelles : l'adresse IP qui vous a été assignée, le début et la fin d'une connexion, avec la date et l'heure, et la quantité de données transmises.

3ème trace : les données personnelles

Sont compris dans les données personnelles : les noms et adresse, l'adresse de facturation et les autres données de contact (téléphone, fax, adresse e-mail). Elles sont enregistrées par votre fournisseur d'accès à Internet.

4ème trace : les protocoles serveur

Aussi bien votre fournisseur d'accès à Internet que l'ordinateur avec lequel vous correspondez enregistrent quand vous êtes en ligne et avec quelle adresse IP. Ces protocoles d'accès sont automatiquement enregistrés dans des historiques de navigation.

5ème trace : l'identification des navigateurs et les liens au sein des navigateurs

Vous pouvez aussi être facilement identifié(e) grâce aux différents navigateurs Internet que vous utilisez — entre autres, grâce aux Add-ons (programmes complémentaires) installés et à vos paramètres personnels. La combinaison unique des informations sur les Add-ons, le système d'exploitation, la résolution d'écran, la langue etc rend chaque navigateur personnel et identifiable.

10 étapes vers l'autodéfense numérique

1. Surfez, si possible, seulement sur des pages sécurisées, dont la ligne d'adresse commence par « https ». Surtout lorsqu'il s'agit de données critiques ou personnelles (coordonnées bancaires, adresse etc.). « Https » signifie « protocole de transmission hypertexte sécurisé » et sert à transmettre les données de manière à ce qu'elles ne puissent pas être interceptées.

2. Désactivez les cookies. Les cookies sont des inscriptions dans des bases de données ou des répertoires pour les échanges d'informations entre les programmes informatiques. Beaucoup de sites internet se font des échanges entre eux à propos de leurs visiteurs. Cela arrive notamment avec les cookies mis sur votre ordinateur par des bannières publicitaires. Paramétrez votre navigateur internet de telle façon qu'il supprime les cookies (cookies http, cookies flash, WebStorage etc) après chaque session.

3. N'utilisez aucun Clouds. Sauvegardez plutôt vos données sur des supports de données, votre disque dur ou votre serveur local. Si vous sauvegardez vos données sur un Cloud ou dans un système de sauvegarde en ligne, ces derniers doivent être cryptés.

4. Imaginez toujours de nouveaux mots de passe. Et il en faut certes que vous pouvez retenir facilement, mais qui ne soient pas faciles à deviner. Utilisez pour cela des chiffres, des majuscules et minuscules, de même que des caractères spéciaux (par ex. %, &, *, /).

5. Installez un programme de messagerie électronique sur votre ordinateur. En écrivant vos e-mails sur votre ordinateur, vous empêchez que chaque mot que vous écrivez soit en ligne simultanément. Ce n'est que lorsque vous envoyez et/ou sauvegardez temporairement votre message que ce dernier va sur Internet.

6. Cryptez vos e-mails et vos SMS. Des programmes simples existent aujourd'hui pour cela. Néanmoins, ce n'est pas d'une grande utilité si vous cryptez vos e-mails mais que le destinataire du message n'utilise aucun cryptage. En outre, seuls le contenu et les pièces jointes sont cryptés, ce qui signifie qu'un lecteur potentiel indésirable sait quand vous avez écrit un e-mail et à qui.

7. Ne chattez pas via des services centraux mais utilisez des fournisseurs indépendants, sur votre ordinateur mais aussi sur votre appareil mobile, de préférence avec le cryptage OTR.

8. Coupez sur votre smartphone la fonction de localisation tout comme sur toutes les plateformes en ligne que vous visitez. Ceci vaut également pour la fonction de reconnaissance faciale.

9. Utilisez le moins possible des services gratuits. Ayez toujours conscience que vous payez alors dans une autre monnaie : avec vos données et votre liberté.

10. Évitez, si possible, les paiements réguliers au moyen des cartes bancaires, des cartes de fidélité dans les transports ou des cartes de réduction, pour empêcher que vos habitudes de consommation ou de voyage ne soient sauvegardées.

Souriez ! Vous êtes observés

Les exemples cités n'en sont que certains parmi d'autres. Vous trouverez des informations supplémentaires en cliquant sur les liens.

Closed Circuit Television (CCTV)
Closed Circuit Television (Télévision en circuit fermé) désigne les installations en vidéosurveillance dont les caméras ne sont liées qu'à un nombre restreint d'ordinateurs et de terminaux et dont les images ne peuvent être vues que par un « public » limité (parmi lesquels la police ou les autorités). Le champ d'action principal de la vidéosurveillance est la surveillance des espaces publics ou privés, du transport et des installations technologiques de toutes sortes.

INDECT
INDECT est un projet de recherche de l'Union Européenne qui a vu le jour en 2009. C'est l'acronyme pour INtelligent information system supporting observation, searching and DEteCTion for security of citizens in urban environment (Système d'information intelligent soutenant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain).
D'après l'UE, INDECT sert, grâce à l'exploitation automatisée des enregistrements vidéo de l'espace public et grâce à la mise en relation de ces derniers avec les informations issues d'internet et d'une multitude de sources de données supplémentaires, à reconnaître les menaces et les actes pertinents du point de vue pénal et à permettre un « travail policier préventif ». En plus de cela, les « comportements anormaux » dans l'espace public sont semble-t-il reconnus dans les images de vidéosurveillance, notamment grâce à des logiciels informatiques.
Sont par exemple classés comme anormaux les comportements suivants : des sessions assises trop prolongées, s'asseoir sur le sol dans les transports publics ou bien perdre son bagage à l'aéroport. Les personnes identifiées comme « suspectes » sur les images de surveillance peuvent être identifiées automatiquement par la reconnaissance faciale assistée par ordinateur et par des drones télécommandés avec caméras de surveillance, et bien sûr poursuivis.
www.indect-project.eu

Echelon — Le réseau d'écoute globale
« Le comité ECHELON affirme que l'existence d'un système d'interception mondial des communications fonctionnant avec la participation des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande ne fait plus de doute. Nous sommes également d'accord sur l'objectif de ce système d'écouter les communications privées et commerciales — et non militaires. » [Rapport du comité ECHELON du Parlement Européen, Gerhard Schmid (SPÖ, Parti social-démocrate autrichien), « Système d'écoute Echelon », Doc. n° A5-0264/2001, Procédure : prise de position non-législative. Discours du 05.09.2001.]
Echelon est un réseau d'écoute et de surveillance qui englobe toutes les communications par satellites — les communications téléphoniques privées ou professionnelles, les communications par fax et les données internet. Les données sont examinées automatiquement par des centres informatiques.
En 2004, un site de la NSA a été fermé dans la ville bavaroise de Bad Aibling sur le soupçon d'espionnage économique contre des entreprises européennes.

ACXIOM
« Acxiom collecte des données à caractère personnel, tels que les noms, adresses, e-mails, numéros de ttéléphone, des données démographiques et socio-comportementales, par le biais de ses questionnaires papier et en ligne, de promotions, ses partenaires commerciaux, des sources publiques, des bases de données commercialisées ainsi que nos sites Web. Les données à caractère personnel peuvent être conservées sous une forme identifiable ou agrégée (de manière à ce que les individus ne puissent pas être identifiés), pour les objectifs définis ci-dessous. » (Acxiom France SAS, Respect de la vie privée).
Acxiom est une entreprise privée qui a cependant aidé le gouvernement américain dans l'élaboration de systèmes après le 11 septembre (voir les derniers reportages du New York Times et du ZEIT). Beaucoup d'activités militaires ou des services secrets (Blackwater, Haliburton) sont maintenant

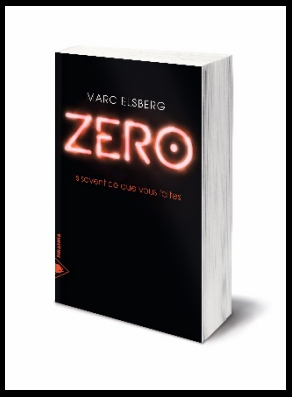
quasiment privatisées. Edward Snowden n'était pas non plus un travailleur de la NSA, mais au contraire employé par l'un des plus gros cabinets de conseil en technologie privés au monde dans ce domaine : Booz Allen Hamilton — et avait, en tant que tel, accès à tous les documents. La séparation entre l'État et le privé n'est donc vraiment pas si facile à discerner.
http://www.acxiom.fr

TEMPORA
Les informations sur TEMPORA proviennent d'Edward Snowden. Tempora est une opération de surveillance des échanges mondiaux en matière de télécommunication et de données internet menées par les services secrets britanniques.
Le programme de surveillance TEMPORA s'appuierait sur deux mesures : la maîtrise d'Internet (Mastering the Internet) et l'exploitation des télécommunications mondiales (Global Telecoms Exploitations). Les e-mails, les posts sur les réseaux sociaux et les informations personnelles des utilisateurs d'internet, ainsi que les conversations téléphoniques, sont surveillés.

PRISM
PRISM est un programme américain et strictement confidentiel de surveillance et d'exploitation des médias électroniques et des données sauvegardées électroniquement. Neuf des plus grands groupes internet et des services des États-Unis seraient impliqués dans ce programme. Les communications internet aussi bien à l'intérieur qu'à l'extérieur des États-Unis seraient surveillées par PRISM. Quant aux informations auxquelles il peut accéder, elles dépendraient de chaque fournisseur internet.

XKEYSCORE
XKEYSCORE (XKS) est un logiciel d'espionnage de la NSA. Il permet aux analystes de parcourir toutes les banques de données possible, et notamment d'analyser les e-mails, les chats en ligne ainsi que l'historique des navigateurs, notamment. Les recherches de toutes sortes peuvent être lancées : numéros de téléphone, adresses e-mail, logins, recherches Google, avec adresse IP, langue et navigateur utilisé. Une identification par adresse IP ou au moyen de la langue utilisée pourrait également être possible.

Marc Elsberg
Zero



PIRANHA
www.piranha.fr