Se protéger sur le Net

Nous pouvons surfer partout dans le monde et nous sommes surveillés par ce biais, nous pouvons être filmés en rue par des caméras de surveillance ou des smartphones dont les vidéos se retrouvent parfois sur un réseau social.

Presque chaque jour, nous sommes confrontés à cet information : vie privée est une des expressions très employée. Il y a une loi vie privé, mais elle offre trop peu de protection dans un contexte international.

Il s'agit des données qui permettent de vous identifier directement ou indirectement, ce sont : votre nom, une photo, un numéro de téléphone ou de compte bancaire, un code, une adresse e-mail voire une empreinte digitale. Elles font de plus en plus l'objet d'un big business. Elles présentent un réel intérêt pour les annonceurs mais aussi pour les autorités… Et les criminels.

Il faut être aussi prudent que possible avec vos données personnelles car surfer sur le net n'a rien d'une activité anonyme. Tout ce qui y passe peut-être enregistré. Lorsque vus achetez sur internet, vos données personnelles sont conservées pour vous envoyer publicités et spams. Des sociétés se sont spécialisées dans le traçage des sites que vous visitez pour vous envoyer des publicités ciblées.

Les mots dès tapés dans un moteur de recherche peuvent eux aussi être traités.

Google – que pratiquement tout le monde connaît a maintenant rassemblé tellement de données sur votre comportement de surfeur qu'il peut vous envoyer des réponses ciblées. Il commence par vous présenter des liens payants et les liens qui suivent sont manipulés en fonction de votre profil de surfeur.

Vous pouvez utiliser des moteurs de recherche comme Duck Duck Go et Blekko.com qui n'analysent pas vos comportements de surfeur, n'enregistrent pas vos clics d'usager, ne conservent pas vos données personnelles et respectent donc mieux votre vie privé.

Si l'enregistrement de notre comportement de surfeur se fait souvent à notre insu, nous-mêmes ne sommes pas toujours des plus discrets. Réfléchissez à deux fois avant de poster textes et photos sur un blog ou sur Facebook ou Twitter, ou Google+. La plupart des réseaux sociaux proposent des paramètres de confidentialité qui permettent de limiter à vos seuls amis l'accès à vos informations. Malheureusement, trop de gens ne savent pas comment ils fonctionnent exactement. Poster une photo pour le regretter immédiatement après peut vous poursuivre longtemps. parce qu'il ne suffit pas d'effacer une donnée sur internet pour la faire disparaître totalement. Les photos peuvent être copiées par des amis, mais aussi des amis d'amis, ou être archivées et réapparaître, par exemple, dans l'historique de Google ou d'un autre moteur de recherche. Pas vraiment sympa quand on sait que les employeurs enquêtent par ce biais sur leurs futurs collaborateurs.

Vous pouvez invoquer le droit à l'image qui découle de la loi sur la protection de la vie privée. Si une personne veut mettre une de vos photos sur son profil, elle doit en principe vous demander l'autorisation. Mais c'est une contrainte bien difficile quand il s'agit d'un site étranger.

Considérez les réseaux sociaux comme de véritables lieux publics et soyez vigilant pour tout ce que vous diffusez via internet.

Masquez votre webcam quand vous ne l'utilisez pas : de plus en plus de hackers peuvent s'en emparer à distance et vous espionner à votre insu. Décochez aussi la case qui indique aux autres utilisateurs que vous avez une webcam.

C'est par les cookies que l'on apprend temps sur vous. Petits fichiers qui s'installent furtivement dans votre ordinateur pendant que vous visitez un site. Ils sont faits par les sites que vous visitez et sont généralement inoffensifs. Mais le problème, c'est que les agences de publicité en font leurs choux gras. La majorité des sites web sont gratuits et vendent des espaces publicitaires et les donnés de leurs clients à ces sociétés qui peuvent à leur tour les revendre et ainsi de suite…

Les hackers utilisent aussi des cookies pour voler vos login et mot de passe qui y sont stockés.

Une option est d'enlever régulièrement les cookies de votre ordinateur mais beaucoup de sites ne vous sont plus accessibles si vous n'autorisez pas les cookies. Vous pouvez aussi faire configurer votre browser (programme de navigation comme Internet Explorer, Firefox…) pour qu'il vous informe de l'installation d'un cookie que vous pouvez alors accepter ou non selon que vous faites confiance au site ou non.

Que votre boîte mail soit envahie de spams pour vous vendre un peu de tout est une chose mais vous n'en subissez pas de préjudice financier. Ce qui peut arriver via la banque par internet. Au début, on essayait surtout d'installer des logiciels malveillants sur votre ordinateur, c'est à dire des programmes qui, comme un espion, tentaient de craquer vos codes.

Aujourd'hui, on a surtout des techniques comme le phishing où on essaye de vous soutirer vos codes, numéros bancaires et mots de passe en vus demandant de répondre à un e-ail ou même par téléphone. Pour en faire, bien sûr, un usage frauduleux. De tels vols ne se font pas que par internet. Les criminels peuvent aussi placer de petites caméras dans les distributeurs automatiques pour enregistrer incognito votre code quand vous retirez de l'argent. C'est le skimming. Depuis l'introduction des puces sur les cartes de paiement, cette fraude est en nette régression mais elle peut encore se produire parce que la majorité des cartes ont une bande magnétique. Par ailleurs, vos données peuvent aussi être copiées lorsque vous donnez un moment votre carte pour paiement.

Ne communiquez jamais de données privées ni votre signature électronique (code réponse) par téléphone ou par e-mail. Si vous avez donné accès à votre ordinateur à des escrocs, déconnectez-le immédiatement et faites une détection complète avec un antivirus mis à jour. Modifiez tous vos mot de passe. Si vous êtes victimes d'une escroquerie, prévenez tout de suite votre banque et portez plainte pour piratage, sabotage d'ordinateur et escroquerie.

Vos données médicales font évidemment partie de vos données personnelles et profitent d'une protection renforcée du fait de leur caractère sensible. Leur traitement ne peut-être fait que par un professionnel de la santé et requiert toujours votre autorisation. les gestionnaires de ces données sont tenus au secret professionnel et ne peuvent donc pas les communiquer à des tiers, même s'il existe des exceptions à ce principe : dans l'intérêt de la santé publique (ex., en cas de maladie contagieuse) ou de la recherche scientifique. Votre médecin traitant peut consulter votre dossier médical électronique, mais uniquement avec votre autorisation. Les pharmaciens peuvent à présent s'échanger des informations sur vos médications (par Ex., dosage), mais avec votre autorisation (que vous pouvez aussi retirer). Ils ne peuvent consulter ces données que sur écran et en présence de leur client.

Les services gouvernementaux utilisent aussi internet pour diverses raisons. Le fisc envoie des rappels pour des arriérés de paiement via Facebook. Est-ce une violation de la vie privée ? Non, selon la commission vie privée. Mais la personne contactée doit être la bonne sans doute possible

sinon on porte atteinte à la vie privée d'une autre personne, homonyme. La conversation doit rester privée : pas question d'afficher le message sur le mur Facebook ou de poster un message sur Twitter. Les services de renseignement et la police sont bien entendu tout aussi intéressés par les informations qui circulent sur internet.

En exécution d'une directive européenne, un nouvel AR exige que tous les opérateurs télécom conservent pendant un an nos communications par téléphone, internet et e-mail pour aider la police et les tribunaux dans leur lutte contre la (cyber) criminalité. Il ne s'agit pas, des contenus des messages mais des données d'identification (nom et adresse), de l'endroit où vous vous trouvez et de la durée de vos visites de sites ou de vos messages téléphoniques ou par e-mail.

Pour être vraiment efficace, la protection de vos données personnelles devrait, dans un environnement aussi transfrontalier qu'internet, être organisée au niveau mondial pour imposer des règles plus strictes aux réseaux sociaux, aux moteurs de recherche et autres services internet. Un projet (de directive), les internautes reçoivent le droit de demander aux services internet d'effacer les données personnelles, les photos ou autres éléments s'ils n'ont aucune raison fondée de les conserver. Elle devrait aussi faciliter l'accès à vos propres données et vous permettre de décider si elles peuvent être utilisées. Si votre autorisation est requise pour les traîter, il faudra aussi vous la demander explicitement. Et si les données stockées sont hackées, le fait devra être immédiatement signalé au contrôleur national. La commission veut également que les paramètres de confidentialité standard deviennent la norme pour les sites des réseaux sociaux et les applications mobile afin que vous ne deviez plus vous-même les mettre en mode sécurité. Avec cet avantage que les mêmes règles vaudront dans toute l'Europe, contrairement à aujourd'hui où les règles différentes s'appliquent selon les pays. Ces règles seront valables aussi pour les entreprises non européennes qui sont actives en Europe, comme Facebook.

Mots de passe : est le premier pilier de la protection contre le piratage. 12345678 se craque en quelques secondes, il faut, disent les spécialistes, 10 mois pour venir à bout de @pEn…@… Plus on combine des lettres, chiffres, majuscules, minuscules et signes spéciaux, mieux on est protégé. A éviter : l'usage des données personnelles comme les prénoms des enfants ou date anniversaire du conjoint qui sont facilement trouvables. Et il est évident que si on utilise le même mot de passe pour tous les sites, pénétrer dans l'un, c'est pénétrer dans tous. Il est aussi recommandé d'en changer régulièrement. Varier les mots de passe – Configurer correctement votre connexion internet et sécurisez votre connexion WIFI pour éviter qu'elle ne soit utilisée par un tiers. – Être prudent avec les supports numériques externes afin d'éviter d'introduire des virus sur votre PC (et inversement) – Ne pas faire confiance aveuglément aux mails que l'on reçoit même d'un expéditeur a priori connu. Faire attention à toujours regrouper l'information. Ne pas demander ou ne pas divulguer d'informations confidentielles par e-mail. – Eviter de trop exposer votre famille et vos-même sur le net. Pour les pirates informatiques, les informations personnelles dispersées sur la toile sont autant de moyens de récolter des indications sur vos mots de passe.

Vous découvrez un site contenant de l'information trompeuse ou vous recevez une proposition frauduleuse par e-mail. Faites un imprimé (pour la preuve) et informez la police locale. Parce qu'on ne peut plus déclarer en ligne les délits constatés sur internet.