6

Protéger sa vie privée sur Internet

CENTRE DE RECHERCHE
SUR L'INFORMATION
SCIENTIFIQUE ET TECHNIQUE
cerist

PROTÉGER SA VIE PRIVÉE SUR INTERNET

Avec l'émergence des blogs et des réseaux sociaux, le nombre d'informations personnelles accessibles en ligne augmente sans cesse. Un nouveau concept est né par analogie à notre environnement naturel, il s'agit de l'intimité numérique et le droit de préserver sa vie privée et ses données personnelles. Dans cette rubrique, nous vous proposons un ensemble de bonnes pratiques pour protéger vos données personnelles sur Internet.

Qu'est ce qu'une donnée à caractère personnel ?

Il s'agit principalement des informations qui permettent d'identifier soit directement, soit indirectement par recoupement d'informations, une personne, telles que :

- nom, prénom,
- photo,
- date de naissance,
- statut matrimonial,
- adresse postale, email, adresse IP d'ordinateur
- n° de sécurité sociale,
- n° de téléphone,
- n° de carte bancaire,
- plaque d'immatriculation du véhicule,
- élément d'identification biométrique,
- les données de géolocalisation
- etc.

L'IDENTITE NUMERIQUE ?

« L'identité numérique d'un individu est composée de données techniques (adresse IP, cookies…), de données personnelles institutionnelles (nom prénom, adresse, n° de tel, certificats…) et informelles (commentaires, notes, billets, photos…). Toutes ces bribes d'information composent une identité numérique plus globale qui caractérise un individu, sa personnalité, son entourage et ses habitudes. Ces petits bouts d'identité fonctionnent comme des gènes : ils composent l'ADN numérique d'un individu ».

ATTENTION SUR INTERNET : TOUT SE GARDE, RIEN NE SE PERD !

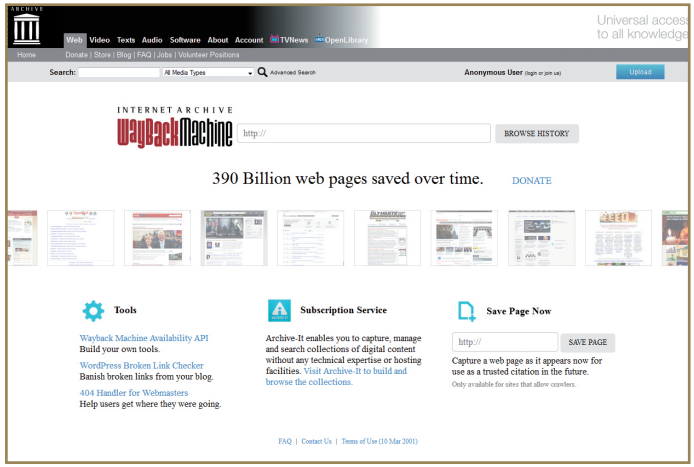
Le Web a une mémoire : toute contribution de votre part sur un site ou un forum par exemple, peut demeurer en ligne pendant des années tant que ce même site est en ligne. Il est également possible de retrouver des archives d'anciennes versions de sites.

Exemple : le site WayBackMachine (Internet Archive) conserve des versions antérieures de pages de sites et blogs depuis 1996.

- Réfléchir avant de publier ou de poster des informations, avis ou photos :

Avant de poster un message ou de diffuser une vidéo ou une photo, sachez que tout ce que vous diffuserez volontairement ayant un caractère privé pourra être visualisé par des milliers de personnes (inconnus) avec le risque que ces contenus soient détournés.

- Protéger vos mots de passe : choisissez des mots de passe compliqués et ne les communiquer à personne.
- Donner le minimum d'informations personnelles sur Internet.
- Vérifier vos traces sur Internet en utilisant un moteur de recherche pour découvrir quelles informations vous concernant circulent sur Internet.
- Prendre le temps de lire les Conditions Générales d'Utilisation avant de s'inscrire sur les réseaux sociaux.
- Sécuriser son compte sur les réseaux sociaux en paramétrant correctement son profil.



- Utiliser un pseudonyme connu seulement de vos proches.
- Prenez garde aux sites qui offrent prix et récompenses en échange de votre contact ou de toute autre information.
- Ne répondez jamais, et sous aucun prétexte, aux spammeurs.

Bonnes pratiques par rapport à l'usage des smartphones pour protéger votre vie privée :

- Ne pas enregistrer dans le smartphone des informations confidentielles telles que des codes secrets (ex : accès à la banque en ligne), des codes d'accès (travail, ordinateur portable) afin de limiter les risques en cas de vol, piratage, ou usurpation d'identité ;
- Mettre en place un délai de verrouillage automatique du téléphone en veille. En effet, en plus du code PIN, ce dispositif permet de rendre inactif (verrouiller) le téléphone au bout d'un certain temps, ce qui empêche la consultation des informations contenues dans le téléphone en cas de perte ou de vol ;
- Activer si possible le chiffrement des sauvegardes du téléphone en utilisant les réglages de la plate-forme avec laquelle le téléphone se connecte. Cette manipulation garantira que personne ne sera en mesure d'utiliser les données figurant dans le smartphone ;
- Installer un antivirus quand cela est possible ;
- Ne pas télécharger d'applications de sources inconnues en privilégiant les plates-formes officielles ;
- Vérifier à quelles données contenues dans le smartphone l'application installée va avoir accès ;
- Lire les conditions d'utilisation d'un service avant de l'installer, et ne pas hésiter à consulter l'avis des autres utilisateurs ;
- Régler les paramètres au sein du téléphone ou dans les applications de géolocalisation afin de toujours contrôler quand et par qui l'appareil peut être géolocalisé ;
- Désactiver le GPS ou le WIFI après utilisation de l'application de géolocalisation.