

## Cliquez, vous êtes fichés !

L'identité numérique

*L'identité numérique, la confidentialité et la sécurité des données personnelles (vie privée, anonymat) sur Internet ou « e-réputation »: les risques, les précautions (outils et méthodologie).*

### Qu'est-ce que l'identité numérique?

#### → Définition

L'évolution des services offerts sur Internet en général et sur le web en particulier amène les internautes à se dévoiler de plus en plus sur les réseaux volontairement ou involontairement. Ces contributions ou traces laissées sur le web, qui peuvent perdurer des années, constituent un reflet virtuel d'une entité physique réelle. C'est un ensemble de données formelles ou informelles constituant une consubstantialité virtuelle d'un individu.

→ Quelles informations personnelles, quelles traces, contributions ou éléments de la vie privée peuvent apparaître sur Internet et via quels usages?

L'importance d'une identité numérique est liée à certains usages qui ne laissent pas apparaître les mêmes types d'informations. Quelques exemples :

– **La souscription auprès d'un FAI (Fournisseur d'accès à Internet) :**

En règle générale, le FAI détient les coordonnées du souscripteur. Il peut tracer l'ensemble des transactions. Il doit également conserver les données de connexion au regard de la législation. La plupart de ces informations sont confidentielles. Cependant, elles existent bien.

– **La connexion :**

Lors d'une connexion sur le réseau, le FAI fournit une adresse IP (numéro qui identifie un ordinateur connecté au réseau) facilement détectable. Grâce à cette adresse, plusieurs informations sont accessibles comme le système d'exploitation et le navigateur utilisés ou la résolution d'écran. Certaines pratiques illégales permettent un accès encore plus étendu.

– **La navigation :**

Certains usages liés à Internet sont propices à la diffusion d'informations personnelles. On peut citer par exemples les sites de rencontres (Meetic...), les plateformes communautaires (Facebook, Myspace...) et les sites de jeux (World Of Warcraft, Secondlife). Notons également que toutes les requêtes effectuées par l'intermédiaire de moteurs de recherche ou méta moteurs sont aussi souvent traçables.

– **La communication :**

Les principaux moyens de communications tels que le courriel, la téléphonie mobile ou la VoIP induisent souvent les utilisateurs à laisser des traces de données sensibles telles que numéros et adresses électroniques.

– **La participation :**

Les commentaires et réactions « postés » sur les blogs, les contributions via la technologie wiki et les avis de consommateurs, pour ne citer qu'eux, sont des pratiques qui laissent apparaître des éléments, qui reconstitués, permettent de déterminer les opinions et centres d'intérêts d'un individu.

– **Les transactions :**

Les certificats (impôts, openid) et les achats en ligne suggèrent la communication de données très sensibles telles qu'identité, adresse physique, numéro de carte

bancaire, etc.

– **Le partage :**

Les sites de partage de photos (Flickr...), de vidéo (Youtube, dailymotion...), de musique et Playlist(Deezer...) ou de favoris (Delicious...) sont sujet à une certaine traçabilité personnelle.

– **La production :**

Les auteurs de sites et/ou blogs sont amenés de façon inhérente à la publication de données. Le fait est d'autant plus marquant pour ceux qui enregistrent un nom de domaine dans la mesure où ils déclarent officiellement des informations d'identité très sensibles qui peuvent être collectées par l'intermédiaire de services tels que « Whois ».

– **Autrui :**

Les propos tenus par d'autres personnes à son sujet sur le réseau de différentes manière permettent également la constitution d'éléments d'identité numérique.

→L'anonymat existe-t-il?

Non. La dissimulation de son identité numérique mérite quelques efforts, l'espionnage et la surveillance en requièrent autant voire plus. Savoir qu'on peut être surveillé ne signifie par forcément qu'on est surveillé. Par exemple, au même titre qu'un véhicule est immatriculé pour circuler, un ordinateur est identifié par son IP lors de sa connexion au réseau. Il convient donc d'être conscient de sa traçabilité sur Internet et d'être prudent.

→Qu'est-ce que « l' e-réputation »?

Certaines personnes ou sociétés ne désirent pas restreindre ou dissimuler leur identité numérique. Bien au contraire, elles cherchent à acquérir une notoriété en contrôlant mais en développant positivement leur identité numérique. D'autres sont calomniées ou diffamées. On peut alors parler d'e-réputation.

Identifier les risques.

Quels sont les usages et les menaces qui peuvent conduire à la divulgation et à la publication d'informations privées ou professionnelles?

→Les malwares

Les malwares constituent une source de risque important. Il existe un large panel de logiciels malveillants en perpétuelle évolution qui ont souvent pour but de collecter des données personnelles confidentielles et sensibles, traquer et surveiller l'utilisateur. On distingue essentiellement comme menaces du type « malware » les virus, les spywares, les vers (worms) ou chevaux de Troie (Trojan).

→Le social engineering et Phishing

C'est un moyen crapuleux usant de persuasion pour extorquer des informations sensibles à l'utilisateur. Le social engineering peut prendre la forme de courriels dits de « phishing » dans le but d'obtenir des renseignements comme un code secret de carte bancaire depuis un faux message prétendument envoyé par une banque.

→Les botnets

Il s'agit d'un réseau d'ordinateurs compromis (à l'insu du propriétaire) dont le but est d'effectuer des opérations de masse parfois malveillantes comme le vol d'informations personnelles ou l'espionnage.

### → Les keyloggers

Ce sont de petits programmes dont la fonction est d'enregistrer et/ou communiquer à un tiers toutes les séquences de touches frappées sur un clavier dévoilant ainsi mots de passe, identifiants, codes secrets...

### → Le hack des services mobile 3G et services en ligne de voIP.

De plus en plus les technologies et services de la téléphonie mobile notamment de la 3G s'apparentent de plus en plus à ceux de l'informatique et du web. Et, à l'instar de la voIP, ils héritent des mêmes faiblesses, risques et autres contraintes.

### → Les FAI

S'il y a bien un partenaire en qui il faut pouvoir faire confiance relativement à Internet c'est le FAI. En effet, lors de la souscription à quelconque forfait ou service auprès d'un FAI, il convient de déclarer des renseignements confidentiels d'identité et bancaires.

### → Les failles de logiciels

De nombreuses attaques extérieures (virus ou spywares) utilisent les failles de logiciels installés sur un ordinateur pour y pénétrer notamment celles du système d'exploitation.

### → Les traces de navigation

Certaines attaques extérieures malveillantes se focalisent sur les traces laissées par une simple navigation anodine sur Internet. Ces éléments peuvent suffire pour collecter des renseignements personnels à des fins malhonnêtes. Parmi ces traces on notera principalement l'historique de navigation, l'historique de téléchargement, les cookies, les identifiants, la mémoire cache de l'ordinateur, les requêtes via moteur de recherche ou la barre d'adresse, les mots de passes enregistrés, les données de formulaires, les favoris (signets ou marques-pages) et le presse-papier.

### → Les Whois (responsables de sites)

Lorsqu'un responsable de site choisi d'enregistrer un nom de domaine, il déclare des informations sensibles qui peuvent être aisément collectées par l'intermédiaire de services « Whois ».

### → Le laxisme lié aux usages et trop de traçabilité.

C'est une erreur de croire qu'on est à l'abri derrière son écran et dire ou faire des choses qu'on ne ferait pas ailleurs que sur Internet. L'empressement, l'insouciance, le clic facile et l'ignorance sont autant d'éléments qui mènent à la divulgation d'informations personnelles.

### → La collecte de données d'identité numérique par un tiers.

Avec un peu de volonté et quelques outils, il n'est pas hors de portée de collecter rapidement quelques informations sur une personne. Il est également important de savoir que tout n'est pas illégal dans la recherche d'informations sur un tiers. En effet, une pratique devenue courante consiste à « Googler » quelqu'un pour en savoir un peu plus sur un individu. Mais attention, certaines pratiques n'en restent pas là, certains opérateurs malveillants utilisent des outils (logiciels, scripts...) plus performants pour reconstituer l'ensemble de l'identité numérique d'une personne.

## Les précautions, les solutions et autres recommandations.

Comportements et outils pour contrôler ou restreindre son identité numérique et/ou la protéger.

### → Pédagogie (enfants)

- Activer un logiciel de contrôle parental.
- Éduquer et prévenir sur les dangers sans diaboliser l'outil.
- Accompagner les plus jeunes dans leur navigation.

### → Matériels et logiciels

- Maintenir à jour le système d'exploitation et autres logiciels de bureautique, navigateur, antivirus, antispywares, pare-feu...
- Verrouiller son ordinateur par un mot de passe.
- Activer le Secure Sockets Layer (SSL) du navigateur.
- Utiliser un compte limité et non administrateur pour la navigation.
- Utiliser les logiciels les plus fiables. Ex: Firefox, Thunderbird, OpenOffice.org.
- Crypter les données sensibles.
- Effectuer des sauvegardes régulières.
- Éteindre l'ordinateur s'il n'est pas utilisé.
- Protéger le réseau sans fil.

### → Comportement lors de la navigation.

- Réfléchir avant de cliquer.
- Utiliser des mots de passe de qualité et les renouveler ou utiliser un fournisseur OpenID fiable.
- Messagerie.
  - Ne pas relayer les canulars ou hoax.
  - Faire preuve de discernement avant d'ouvrir une pièce jointe.
- Ne pas être avare de preuves pour vous assurer de la crédibilité de vos interlocuteurs.

### → Prévention

- Mettre en garde son entourage sur la diffusion d'informations privées.
- Vérifier soi-même l'étendue de son identité numérique pour mieux la contrôler (alertes Google par mots-clés).

### → Garder un esprit critique

- Veiller au respect des lois et ne pas hésiter à se défendre le cas échéant.
- S'informer sur les outils et méthodes toujours en évolution.
- Participer au débat, signaler à la communauté tout élément susceptible de servir le plus grand nombre.
- Rester réaliste, l'anonymat n'existe pas plus que dans son véhicule qui porte une plaque d'immatriculation.

## En conclusion

Il ne faut pas sombrer dans la paranoïa, tout un chacun n'est pas la cible d'une enquête approfondie au quotidien. Mais rester réaliste et même savoir faire preuve d'un peu de futilité, l'anonymat n'existe pas sur Internet. Que l'on fasse le choix de la discrétion ou de l'e-réputation, il n'y a rien d'insurmontable tant qu'on observe rigueur et veille.

Sources et références :

[securite-informatique.gouv.fr](http://securite-informatique.gouv.fr)

[internet101.ca](http://internet101.ca)

[cnil.fr](http://cnil.fr)

[ssi.gouv.fr](http://ssi.gouv.fr)

[webaverti.ca](http://webaverti.ca)

[mineurs.fr/citoyens](http://mineurs.fr/citoyens)

[monidentite.isiq.ca](http://monidentite.isiq.ca)

[internetsanscrainte.fr](http://internetsanscrainte.fr)

[clusif.asso.fr](http://clusif.asso.fr)

Risques:

[securite-informatique.gouv.fr/rubrique10.html](http://securite-informatique.gouv.fr/rubrique10.html)

[cnil.fr/index.php?id=19](http://cnil.fr/index.php?id=19)

[bugbrother.blog.lemonde.fr/2009/01/16/tout-ce-que-vous-avez-toujours-voulu-savoir-sur-moi-mais-que-vous-aviez-la-flemme-daller-chercher-sur-linternet](http://bugbrother.blog.lemonde.fr/2009/01/16/tout-ce-que-vous-avez-toujours-voulu-savoir-sur-moi-mais-que-vous-aviez-la-flemme-daller-chercher-sur-linternet)

[dslvalley.com/vie+privee+sur+internet+les+cnil+sonnent+l+alerte-18-11-2008.html](http://dslvalley.com/vie+privee+sur+internet+les+cnil+sonnent+l+alerte-18-11-2008.html)

[cyberzoide.developpez.com/securite/indiscretions-navigateur/](http://cyberzoide.developpez.com/securite/indiscretions-navigateur/)

[lexpress.fr/actualite/high-tech/le-portrait-google-qui-met-le-feu-a-la-toile\\_732230.html](http://lexpress.fr/actualite/high-tech/le-portrait-google-qui-met-le-feu-a-la-toile_732230.html)

[cases.public.lu/fr/risques/2008/SANS/index.html](http://cases.public.lu/fr/risques/2008/SANS/index.html)

[lemonde.fr/technologies/article/2009/01/17/un-internaute-piege-par-ses-traces-sur-la-toile](http://lemonde.fr/technologies/article/2009/01/17/un-internaute-piege-par-ses-traces-sur-la-toile)

Solutions

[securite-informatique.gouv.fr/gp\\_rubrique34.html](http://securite-informatique.gouv.fr/gp_rubrique34.html)

[cnil.fr/index.php?id=125](http://cnil.fr/index.php?id=125)

[internet101.ca/fr/techtips.php](http://internet101.ca/fr/techtips.php)

[webaverti.ca/french/PrivacyInvasions.aspx](http://webaverti.ca/french/PrivacyInvasions.aspx)

[epn-ressources.be/10-conseils-pratiques-pour-protger-votre-vie-privee-sur-internet](http://epn-ressources.be/10-conseils-pratiques-pour-protger-votre-vie-privee-sur-internet)

[monidentite.isiq.ca/suivez\\_bonnes\\_pratiques](http://monidentite.isiq.ca/suivez_bonnes_pratiques)

[cases.public.lu/fr/pratique/comportement/index.html](http://cases.public.lu/fr/pratique/comportement/index.html)

Jeux pédagogiques

[protegetonordi.com](http://protegetonordi.com)

[pointdecontact.net/famille/](http://pointdecontact.net/famille/)

[codeluweb.aol.fr/](http://codeluweb.aol.fr/)

L'identité numérique

[mashable.com/2009/01/18/gerer-sa-presencereputation-sur-le-web-social](http://mashable.com/2009/01/18/gerer-sa-presencereputation-sur-le-web-social)

[wikipedia.org](http://wikipedia.org)

[fredcavazza.net/2006/10/22/qu-est-ce-que-l-identite-numerique/](http://fredcavazza.net/2006/10/22/qu-est-ce-que-l-identite-numerique/)

[a-brest.net/article1841.html](http://a-brest.net/article1841.html)

[usernamecheck.com/](http://usernamecheck.com/)

[api-exploration.net/mashups/ePassport/](http://api-exploration.net/mashups/ePassport/)

[ed-productions.com/leszed/index.php?identite-numerique](http://ed-productions.com/leszed/index.php?identite-numerique)

[wikipedia.org/wiki/OpenID](http://wikipedia.org/wiki/OpenID)