

Reprendons le contrôle de notre vie privée sur Internet

Genma

September 23, 2015





A propos de moi

Où me trouver sur Internet?

- Le Blog de Genma :
<http://genma.free.fr>
- Twitter :
<http://twitter.com/genma>

Mes projets-contributions

Plein de choses dont:

- Des conférences sur plein de thèmes différents


Le Blog de Genma


Rencontre avec Genma IRL.

publié le 3 août 2013 par Genma

Si tu es un festuc régulier de ce blog, que ça bouille dans ton ventre, pour manger Genma un resto n'est tout simplement pas délicieux, comme moi que l'on va faire un rendez-vous. En effet, je serai disponible du vendredi 11 août au Mardi 20 août, en fin de journée ou le soir, à l'horizon où tu veux bien, sur Paris, France. Si tu es partant, fais signe... A la suite de cette rencontre, je pourrais faire (ou non), si tu t'en assois, un petit retour rendu sur mon blog, avec une quote (...)

POUR LIRE LA SUITE... [Facebook](#) [Twitter](#) [Email](#)



Lifehacking - L'importance du matériel

publié le 2 août 2013 par Genma

Un bon ordinateur doit avoir de bons outils pour faire du bon travail. Un meilleur matos ne sera pas assez bon si son instrument de musique n'est pas de qualité. Il en est de même pour l'informatique. Ce n'est pas la taille ou le poids.

en fait il y a deux écrans, sur ma machine prédictive, j'avais pour travailler du birdien, un écran 22" et un écran 17" (celui du portable), un surtasseur de l'autre. Avec ma nouvelle machine, je vais passer sur un unique écran de 17", avec un PC plus lent (je ...)

POUR LIRE LA SUITE... TAGS : [Lifehacking](#)

[Facebook](#) [Twitter](#) [Email](#)

Syndication
 [RSS](#) [Atom](#)

shearwater



Date de mise à jour : [Le 3 août 2013](#)

Rechercher : [Chercher](#)

Commentaires [Ajouter un commentaire](#)

OK

Catégories
[Actualités Geek de la semaine](#)
[Blog : tout et rien](#)

Internet, c'est quoi?

Internet, un réseau de réseau

- Internet c'est un réseau de réseau d'ordinateurs connectés entre eux.
- Il y a d'un côté les serveurs, des gros ordinateurs, sur lesquels il y a des sites Internet.
- Et de l'autre, il y a "nous", avec notre PC, notre tablette, notre smartphone...

Toutes ces traces qu'on laisse
sur Internet... sans le savoir

Les traces de navigation *locales*

Quand on va sur *Internet*

Plein de fichiers sont créés :

- Historique des pages visitées,
- Données saisies dans les formulaires et barres de recherche,
- Les mots de passe conservés,
- La liste des téléchargements,
- Les cookies,
- Les fichiers temporaires...)

Tout ce que l'on fait depuis son navigateur, est, par défaut, conservé sur notre ordinateur, tablette, smartphone...

Les logs de connexions

Les traces laissé sur les sites Internets

Les serveurs Internet gardent différentes traces dont :

- l'Adresse IP
- les heures et dates de connexions
- les informations saisies...
- le navigateur, son modèle, le système d'exploitation...

Les traces écrites

Sur les réseaux sociaux, les blogs, les forums...

Sur tous ces comptes que l'on en a en ligne :

- On commente, on réagit ;
- On "like" ;
- On ajoute des photos, des vidéos.

Ce sont autant de traces que l'on peut lier à nous.

L'image que je donne de moi

Googler "son nom"

- Les résultats apparaissant sont-ils bien ce que l'on souhaite?

[Le Blog de Genma ...](#)

[genma.free.fr/](#) ▾

Interview de Skhaen, Telecomix et Cyphercat.eu. publié le 13 septembre 2013 par **Genma**. C'est via sa conférence à PSES2012, traitant de la cryptographie et ...

[Genma \(genma\) on Twitter](#)

[https://twitter.com/genma](#) ▾

The latest from **Genma** (@genma). **Genma** - Compte Officiel ;-) - Un peu linuxien, un peu otaku mais surtout Geek et Blogueur sur Le Blog de **Genma**. Paris.

[Genma Kun - France | LinkedIn](#)

[fr.linkedin.com/in/genma](#) ▾

Région de Paris , France - Geek, Blogueur, Développeur, Lifehacker

Voir le profil professionnel de **Genma** Kun (France) sur LinkedIn. Grâce à LinkedIn, le plus grand réseau professionnel au monde, les professionnels comme ...

[Genma Kun | Facebook](#)

[https://www.facebook.com/genma](#) ▾

Genma Kun is on Facebook. Join Facebook to connect with **Genma** Kun and others you may know. Facebook gives people the power to share and makes the ...

Adage

Les paroles s'envolent, les écrits restent

- Cet adage est encore plus vrai avec Internet.
- Il faut partir du principe que ce que l'on dit sera toujours accessible, même des années après.
- Tout ce qui est sur Internet est public ou le sera (même si c'est "privé". Les conditions d'utilisation évoluent. cf. Facebook).

Rq : Il ne faut donc pas abuser de la liberté d'expression et rester respectueux des lois en vigueur.

Les mails - courriers électroniques

Un mail que l'on envoie, c'est une carte postale

"On" sait

- qui écrit à qui ;
- quand ;
- pour se dire quoi.

Ex : Gmail lit le contenu des mails pour afficher de la publicité ciblée.

Le facteur peut lire la carte postale

"On" peut

- envoyer un mail au nom de quelqu'un d'autres ;
- lire les mails qui circulent sur un réseau...

Les données qui transitent *en clair* sur le Web

Quand on consulte un site Internet

Le site Internet sait :

- D'où l'on vient (pays, adresse exacte)
- La langue que l'on parle, l'heure de l'ordinateur, son modèle...

Les connexion http

Sans le "cadenas" dans la barre d'adresse :

- Le mot de passe circule "en clair"
- Avec *un logiciel, un pirate* peut récupérer le mot de passe.

Cloud - l'informatique dans les nuages

Définition du cloud

- Le *Cloud*, c'est l'ordinateur d'un autre.



Les problèmes du cloud

Le stockage est gratuit

- les documents sont analysés (pour de la publicité, de l'espionnage industriel... etc.).
- Nos données peuvent être piratées et diffusées dans la nature?
- Si le service ferme, que deviennent nos données?

Les métadonnées

Ces données cachées des documents

Les métadonnées

Qu'est-ce qu'une métadonnée ?

Une métadonnée est une information qui caractérise une donnée.

Prenons un exemple : lorsque vous créez un PDF, en général, des données additionnelles sont ajoutées à votre fichier : le nom du logiciel producteur, votre nom, la date de production, la description de votre document, le titre de votre document, la dernière date de modification, ... ce sont des métadonnées.

Vous n'avez peut-être pas envie de partager ces informations lorsque vous partagez votre fichier.

Metadata Photo

Propriétés de 009 2011 Mars Japon Kyoto.jpg	
	Général Permissions Ouvrir avec Image
Type d'image	jpeg (Le format d'image JPEG)
Largeur	2048 pixels
Hauteur	1536 pixels
Marque de l'appareil photo	Canon
Modèle de l'appareil photo	Canon PowerShot S5 IS
Date du cliché	2011:03:04 22:46:52
Temps de pose	1/15 sec.
Ouverture focale	3,34 EV (f/3,2)
Vitesse ISO	200
Flash déclenché	Flash did not fire, compulsory flash mode
Mode de mesure	Motif
Distance focale	11,1 mm

Metadata Photo

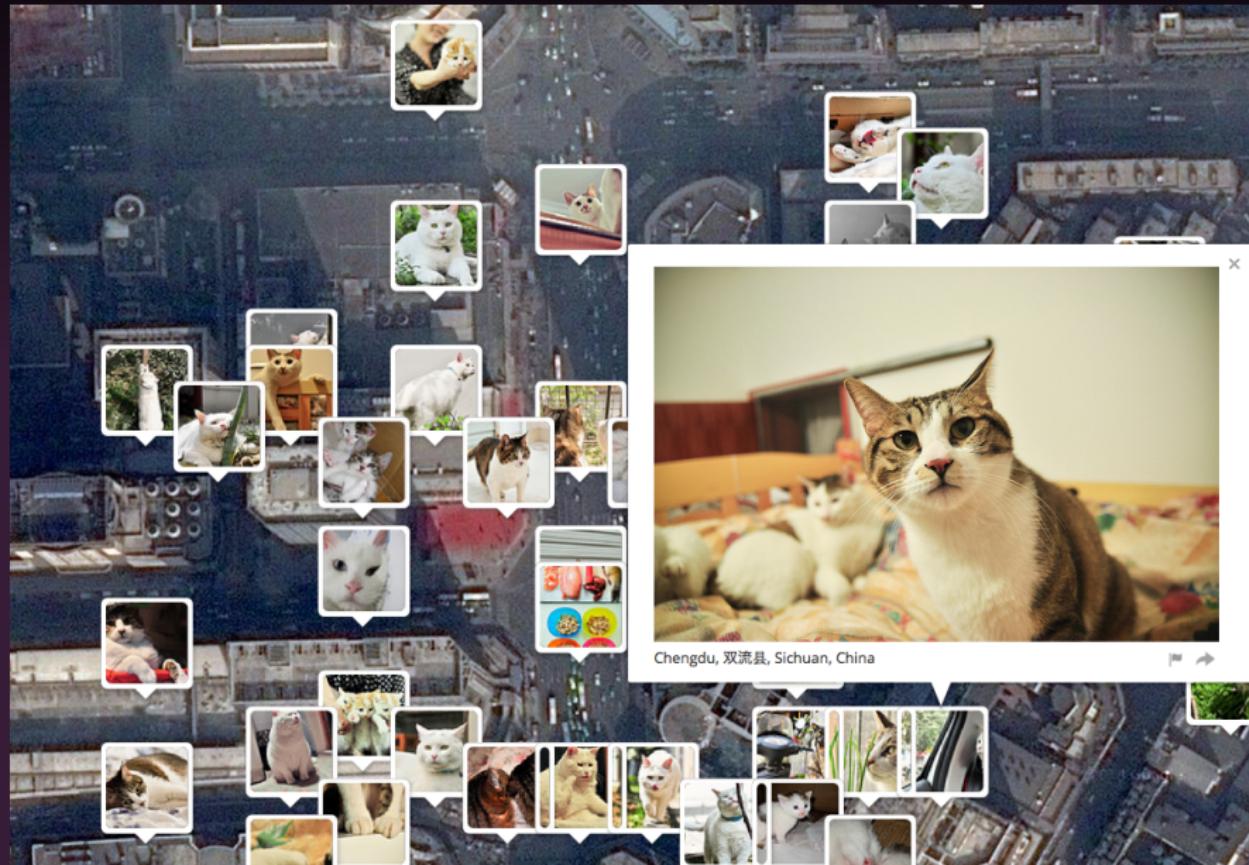


Exif Toolbox

Properties

Equip Make: Canon
Equip Model: Canon EOS 450D
Orientation: 1
X Resolution: 72/1
Y Resolution: 72/1
Resolution Unit: 2
Date Time: 2008:09:06 13:23:53
YCbCr Positioning: 2
Exposure Time: 0
F-Number: F/10
ISO Speed: ISO-400
Longitude: 36.165597
Latitude: 69.960251
DTOrig: 2008:09:06 13:23:53
DTDigitized: 2008:09:06 13:23:53
CompConfig: -
Shutter Speed: 1/196.72
Aperture: F/9.92
Exposure Bias: 0/1
Metering Mode: Pattern
Flash: reserved
FocalLength: 30
Maker Note: -

Géolocalisation des chats



Metadata Word 1/2

Général Personnaliser Résumé

Propriété	Valeur
Description	
<input checked="" type="checkbox"/> Titre	Titre du document
<input checked="" type="checkbox"/> Objet	Sujet du Document
<input checked="" type="checkbox"/> Catégorie	Confidentiel
<input checked="" type="checkbox"/> Mots-clés	Confidentiel, Secret Defense
<input type="checkbox"/> Modèle	Normal.dot
<input type="checkbox"/> Pages	1
<input type="checkbox"/> Nombre de mots	11
<input type="checkbox"/> Nombre de caractères	68
<input type="checkbox"/> Nombre de lignes	6
<input type="checkbox"/> Nombre de paragraphes	1
<input type="checkbox"/> Échelle	Non
<input type="checkbox"/> Liens brisés ?	0
<input checked="" type="checkbox"/> Commentaires	Ce document est secret d...
Origine	
<input checked="" type="checkbox"/> Auteur	Auteur
<input type="checkbox"/> Dernier enregistrement	

<< Simple

OK Annuler Appliquer

Metadata Word 2/2

Général Personnaliser Résumé

Propriété	Valeur
<input type="checkbox"/> Pages	1
<input type="checkbox"/> Nombre de mots	11
<input type="checkbox"/> Nombre de caractères	68
<input type="checkbox"/> Nombre de lignes	6
<input type="checkbox"/> Nombre de paragraphes	1
<input type="checkbox"/> Échelle	Non
<input type="checkbox"/> Liens brisés ?	0
<input checked="" type="checkbox"/> Commentaires	Ce document est secret d...

Origine

<input checked="" type="checkbox"/> Auteur	Auteur
<input type="checkbox"/> Dernier enregistrement	
<input checked="" type="checkbox"/> Numéro de révision	22
<input checked="" type="checkbox"/> Nom de l'application	Microsoft Office Word
<input checked="" type="checkbox"/> Entreprise	La société
<input type="checkbox"/> Date de création	06/01/2014 14:56
<input checked="" type="checkbox"/> Date du dernier enregi...	06/01/2014 15:05
<input type="checkbox"/> Heure de modification	01/01/1601 01:07

<< Simple

OK Annuler Appliquer

Les métadonnées

Pourquoi les métadonnées sont elles un risque pour notre vie privée?

Les métadonnées dans un fichier peuvent en dire beaucoup sur vous.
Les appareils photos enregistrent des données sur le moment où une photo a été prise et quel appareil photo a été utilisé.

Les documents bureautiques ajoutent automatiquement l'auteur et diverses informations sur la société aux documents et feuilles de calcul.

Peut-être que vous ne voulez pas divulguer ces informations sur le web?

Quand on fait une recherche
dans Google...

Google

Découvrez comment Google vous voit

Google tente de créer un profil de base de vous, selon votre âge, votre sexe, vos centres d'intérêt. C'est avec ces données que Google vous « sert » des annonces pertinentes. Vous pouvez examiner la façon dont Google vous voit ici : <https://www.google.com/ads/preferences/>

Découvrez l'historique de votre géolocalisation

Si vous utilisez Android, votre appareil mobile peut envoyer à Google des informations de géolocalisation et de vitesse de déplacement d'un point à l'autre. Vous pouvez voir l'historique complet de vos « positions » et les exporter ici :

<https://maps.google.com/locationhistory>

Google

Découvrez l'intégralité de votre historique de recherches Google

Google enregistre jusqu'à la moindre recherche que vous faites. Par-dessus le marché, Google enregistre toutes les pubs Google sur lesquelles vous avez cliqué. L'historique est à votre disposition ici :

<https://history.google.com>

Découvrez tous les appareils qui ont accédé à votre compte Google

Si vous craignez que quelqu'un d'autre ait pu utiliser votre compte, vous pouvez trouver la liste de tous les appareils qui ont accédé à votre compte Google, leur adresse IP et leur emplacement approximatif :

<https://security.google.com/settings/security/activity>

Découvrez toutes les applications et les extensions qui ont accès à vos données Google

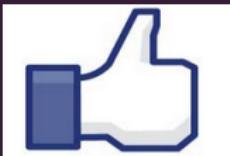
Ceci est une liste de toutes les applications qui ont tout type d'accès à vos données. Vous pouvez voir le type exact de permissions accordées à l'application et révoquer l'accès à vos données en suivant ce lien :
<https://security.google.com/settings/security/permissions>

Sur Internet, si c'est gratuit,
c'est VOUS le produit

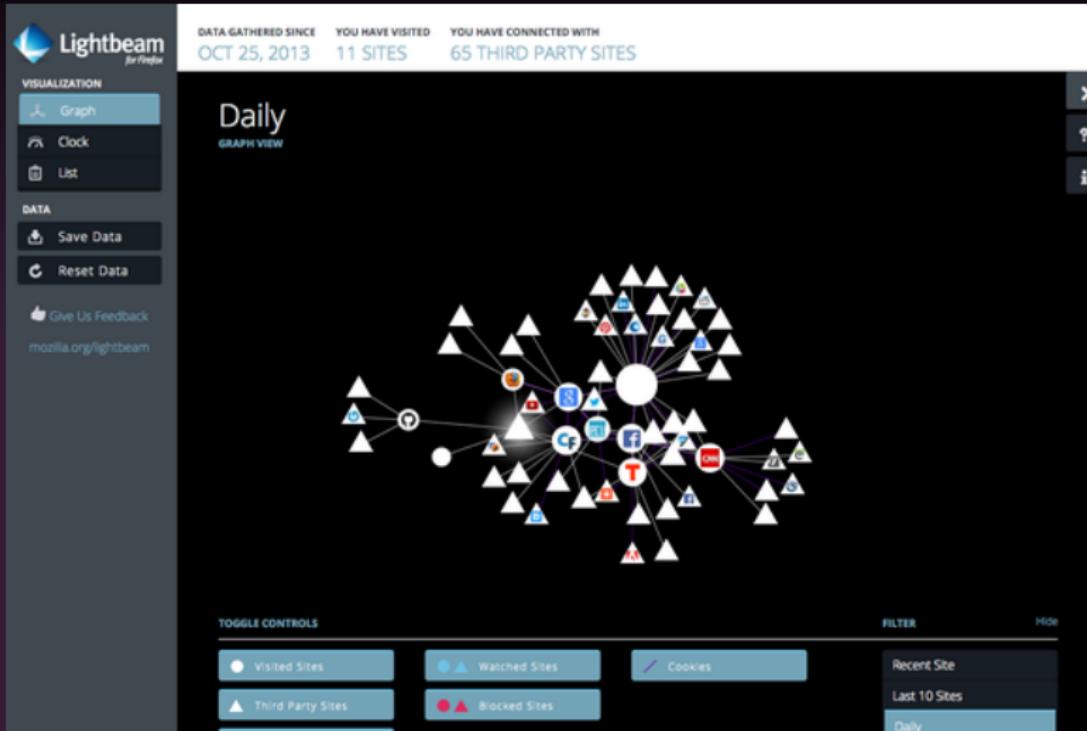
Comment est-on pisté?

Toutes les publicités nous espionnent

- Le bouton Like de Facebook : il permet à FaceBook de savoir que vous avez visité ce site, même si vous n'avez pas cliqué sur ce bouton.
- Même si vous vous êtes correctement déconnecté de Facebook.
- De même pour le bouton le +1 de Google, les scripts de Google Analytics,
- Tous les publicité, Amazon...



Lightbeam



Comment se protéger ?
Un peu d'hygiène numérique

Navigateur

Utilisez un navigateur respectueux de nos données personnelles : Firefox.

Pourquoi Firefox?

- La navigation privée permet de ne pas garder de traces sur l'ordinateur (mais ça ne suffit pas).
- On peut ajouter des extensions anti-tracking et anti-pubs (Ghostery/Request Policy, Adblock...)

Installer des extensions pour Firefox

AdBlock - block 1/2

Page avec publicité :

Screenshot of a Mozilla Firefox browser window showing the 01net website.

The title bar reads: "01net - informatique high-tech : actu, produits, téléchargement logiciels et jeux - Mozilla Firefox".

The menu bar includes: Fichier, Édition, Affichage, Historique, Marque-pages, Outils, and a question mark icon.

The address bar shows the URL: "www.01net.com".

The main content area features a large banner for the "DOSSIER iPad 5" with a "J'Y VAIS" button. The banner also includes the 01net logo, a photo of three iPads, and a "numericable" logo.

A sidebar on the left says: "Retrouvez toutes les informations sur la conférence Apple" with a "J'Y VAIS" button.

The navigation menu at the top of the page includes: ACTUALITÉS, COMPARATIFS ET TESTS, JEUX, ASTUCES, VIDÉO, telecharger.com, BONS PLANS, FORUM, 01BUSINESS, and 01MEN.

The main article headline is: "iPad Air et iPad mini Retina: les premières prises en main en vidéo". It includes a thumbnail image of two iPads and a play button.

On the right side, there's another "iPad Air et iPad mini Retina: les premières prises en main en vidéo" section with a thumbnail and a timestamp: "23/10/2013 à 09:30".

At the bottom right, there's a video player showing two men talking, with the caption: "Apple, Nokia, Microsoft : rendez-vous ce soir pour un grand show".

AdBlock - Microblock 2/2

Bloque les publicités. Allège les pages.

01net - informatique high-tech : actu, produits, téléchargement logiciels et jeux - Mozilla Firefox

Fichier Édition Affichage Historique Marque-pages Outils ?

01net - informatique high-tech : actu, produ... +

www.01net.com

nos newsletters nos magazines

01net Lisez 01net pour 2,45 € / m² seulement

◀ ▶ 🔍 W Wikipédia (fr)

01net

Rechercher un logiciel OK

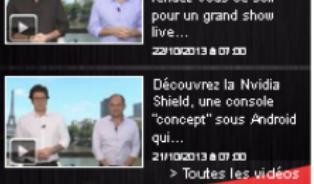
ACTUALITÉS COMPARATIFS ET TESTS JEUX ASTUCES VIDÉO telecharger.com BONS PLANS FORUM 01BUSINESS 01MEN

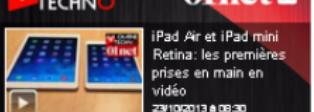
 iPad Air et iPad mini Retina: les premières prises en main en vidéo

Apple a dévoilé hier soir deux nouvelles tablettes: un iPad Air plus fin et plus léger, ainsi qu'un iPad mini avec écran Retina. 01net vous livre son impression, produits à l'appui.



 01net APPROUVE

 Découvrez la Nvidia Shield, une console "concept" sous Android qui... 21/10/2013 à 07:00 > Toutes les vidéos

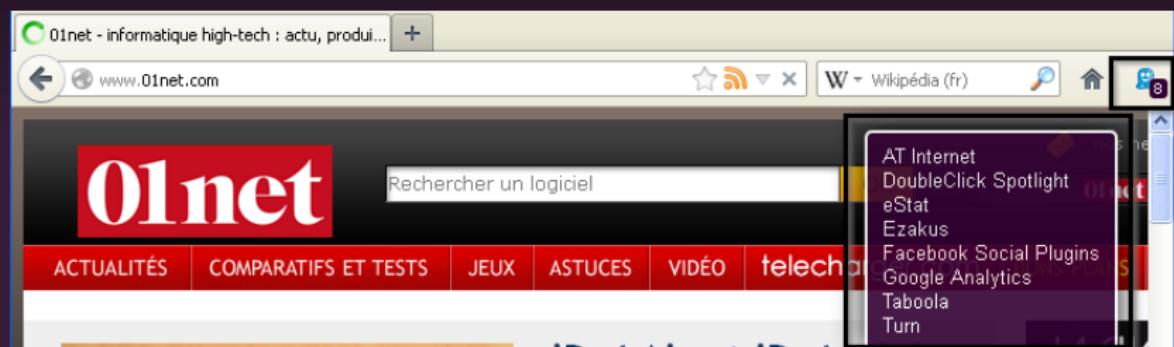
 iPad Air et iPad mini Retina: les premières prises en main en vidéo 23/10/2013 à 08:30

 Apple, Nokia, Microsoft : rendez-vous ce soir pour un grand show live... 22/10/2013 à 07:00

TOP TESTS

Ghostery

Bloque tous les trackers associés au site.



Https Everywhere

Avoir une connexion httpS dès que possible

The screenshot shows the homepage of the EFF's HTTPS Everywhere project. At the top, the EFF logo and the text "ELECTRONIC FRONTIER FOUNDATION DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD" are visible. Below this is a red navigation bar with links for "HOME", "ABOUT", "OUR WORK", "DEEPLINKS BLOG", and "PRESS ROOM". The main content area features a large graphic of a blue padlock with arrows pointing towards it, next to the text "HTTPS Everywhere". Below this, there are several links: "HTTPS Everywhere", "FAQ", "Report Bugs / Hack On The Code", "Creating HTTPS Everywhere Rulesets", "How to Deploy HTTPS Correctly", and "HTTPS Everywhere Atlas". To the right of these links is a large Firefox logo with the text "Install in Firefox".

ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME ABOUT OUR WORK DEEPLINKS BLOG PRESS ROOM

HTTPS Everywhere

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure.
Encrypt the web: [Install HTTPS Everywhere today.](#)

FAQ Report Bugs / Hack On The Code Creating HTTPS Everywhere Rulesets How to Deploy HTTPS Correctly HTTPS Everywhere Atlas

Install in Firefox

Utiliser des moteurs de recherche plus respectueux de la vie privée (DuckDuckGo...)

Les alternatives à Google

- Duckduckgo <https://duckduckgo.com>
- Qwant <https://www.qwant.com>
- Framabee <https://framabee.org> ou TontonRoger
<https://tontonroger.org/>

Duckduckgo - Google tracks you. We don't.

<https://duckduckgo.com/>



DuckDuck**Go**

 A white search bar with a green rectangular button containing a white magnifying glass icon to its right. To the right of the button is a small vertical dropdown menu icon.

Chercher incognito. Trouver illico.

Différents modèles de menace

Répondre aux questions

- Quelles sont les données et informations que j'estime personnelles - confidentielles?
- Qu'est ce que je suis près à apprendre et à faire pour les protéger?

Autres conseils

Utiliser un pseudonyme

Le pseudonymat

Définitions

- Contraction des termes pseudonyme et anonymat, le terme de pseudonymat reflète assez bien la volonté contradictoire d'être un personnage public et de rester anonyme...
- Un pseudonyme, c'est aussi une identité publique, qui est associée à un ensemble cohérent de compte qui forme un tout : un blog, un compte Twitter, un compte Facebook...

Avoir un pseudonyme ne veut pas dire faire et dire n'importe quoi.

Il en va de l'image que je renvoie, que je donne de moi et de ma crédibilité présente et à venir.

Les avantages du pseudonymat

Ce que permet le pseudonymat

Il permet de cloisonner sa vie numérique.

- On a une identité civile en ligne (nom prénom) avec le strict minimum.
- Et une identité publique, un pseudonyme, qui permet d'avoir une activité plus fournie.

Ne pas oublier d'avoir une adresse mail qui n'est pas de la forme prénom.nom (sinon on perd l'intérêt du pseudonyme).

Plusieurs pseudonymes

Quand on crée un compte sur un site, on peut envisager de saisir des informations nominatives spécifiques à ce site. On aura alors un pseudonyme par type de communauté fréquenté (jeu vidéo, informatique, de rencontres...).

Si il y a un problème (*compte piraté*), on limitera le risque de diffusion des informations personnelles.

Pseudonymat et célébrité

Nombreux sont les célébrités du monde de la télévision, cinéma, musique... Et Internet?

Des pseudonymes internet *connus*

- Maitre Eolas, l'avocat
- Zythom, l'expert judiciaire
- Boulet, dessinateur
- ...

Et beaucoup d'autres, dans les communautés geek, hackers...

Les limites du pseudonymat

Un pseudonymat c'est contraignant

On est très facilement tracés et reliés à sa véritable identité (via l'adresse IP).

- Pour avoir un pseudonymat parfaitement cloisonné, il faut utiliser différentes techniques avancées...

NE JAMAIS faire d'erreur

- On ne dévoile pas son pseudonyme a des personnes qui connaissent notre identité civile.
- On ne dévoile pas son visage en publicue....

Le pseudonymat est donc on ne peut plus relatif et tout dépend de ce que l'on souhaite comme pseudonymat.

Une solution simple reste d'être
moins *bavard*

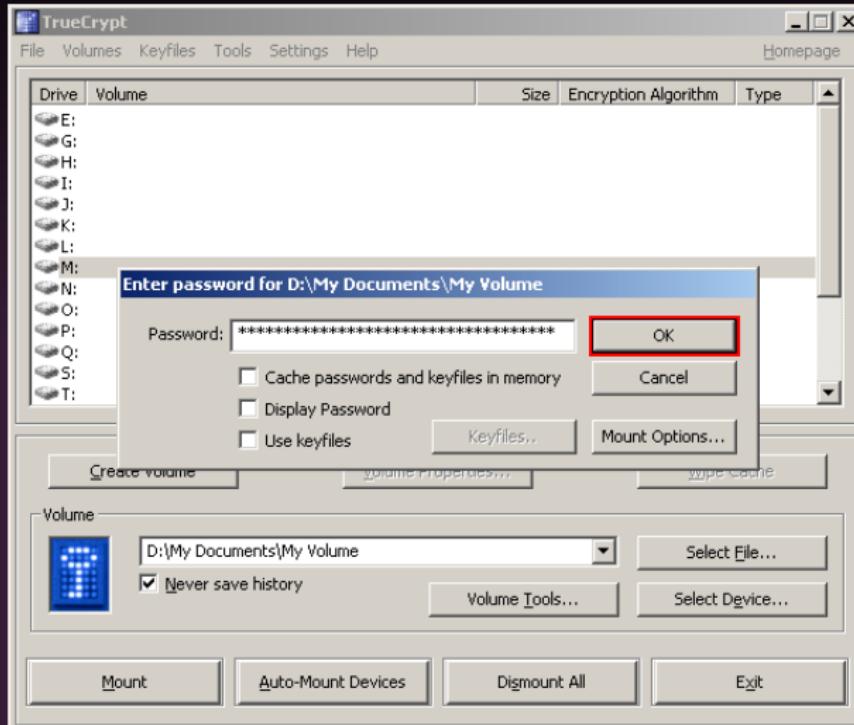
D'un peu plus complexe...
à très technique



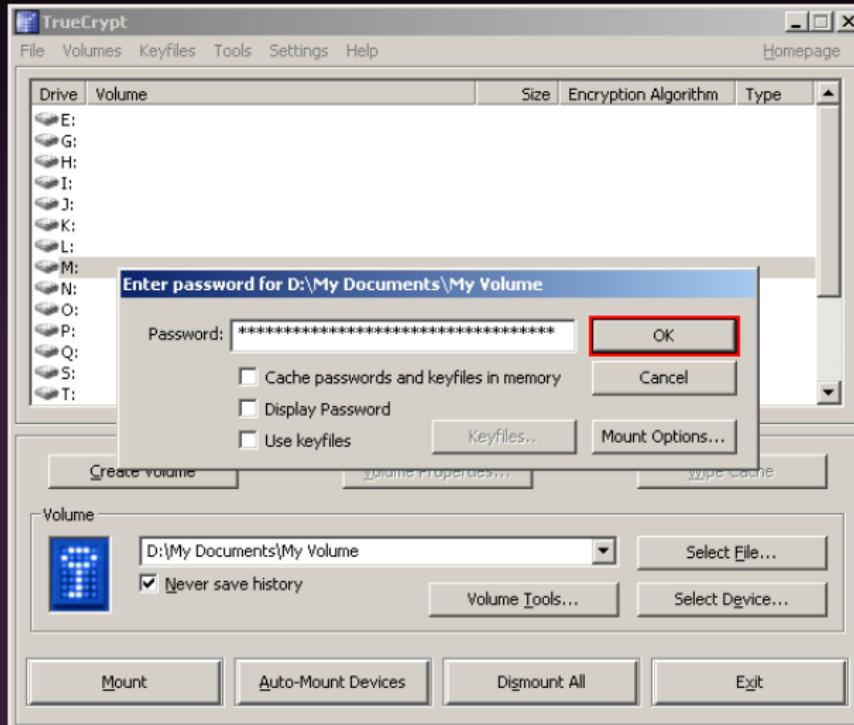
Café *vie privée*

Chaque exemple cité après, c'est entre 1h à 3h d'ateliers...

Chiffrer ses disques durs (TrueCrypt...)



Chiffrer ses disque durs (TrueCrypt...)



Chiffrer ses mails (GPG...)

De Fragment

MP

genma

MP

Re:

Expéditeur: MP

À genma

-----BEGIN PGP MESSAGE-----
Charset: windows-1252
Version: GnuPG v2

hQIMA3PPp34hoQrHAQ#F86rW3I3ShEJVGzEkNvbTnyNpXsY9bO37+rHkLTgtVW4
oleE3lOFtk3t5Ew3Xs8NDmEN1hn25VpHA4dYFvWq0Dkqn6wCenO4VX5injs9TsBb/
KeF1Hq+8yT6tCqMPTB9cjYycVvf6OUPfmo8568Di53WSBjB17jv9p30SQTjdStMD
opekj34bHz+coNMuj7DCntGVW1zuLzB7H21pfcb2kiSTRVVR5DY2M7ISIs85U8e
J0kGa+Wh4z88MB/nRsqQISjmfZf7nAl1MDphuMCH6avkfGPRN0voqKNYTwiR/qgA
bky2odLn5qb1Mf2fekwABOTTb09cy7CnjBkiglibNOMCDUwoMVZHDmwbh7gCzeFz
B5CkNwBKryEjj5dass8KocUbkGJVcq8RL2+T5GXK/X/2qp/2DxF8RQOlbyDEoMnBc
2ee1jGwkcnHPZjTmZyKyNd12AcLJ80MfgNtIvwJGatvhz7Pu5kq9txkvysm79PiQ
dBn1lFPC1EtCFc1gBQ4fc2Tg8nNgvHcmuVJW/zv5H7A+vuh4zktptYIk26
GVh0FcZYyArv2+ciywCsWpDTVityqukuARmxp12KnEKdhPrx97+Publ1V0/mbo+f
kga6Xp/gDQCscrYR5wbjAIUFAYN9v/xUOnwVdp59rMhI+1iApmrRqgRnlBwW+F
AgwdXZBqHjgnacBD/9cdls0415wlrtHSLo/16rw686gpjH6SEYaBqDwWzlsH4lk
jGszCpXBAnIEMNqr8Hd6ozcW/hYTb2LcB23S0up4FQJQRmPjAdWj/MJodvzypl6
ADTjb8mbu5LrzS3x6s7sgavzfCcNMe9FJRCBGW+U2p+ItnvxR81Xgx+eyQ4dj3PO
HRAlysDeu4EmBccugZQ3FKykcCcBa/rBodjFiwyEsciBCmC2iX0EycWKmY7GobR
vTd+N6AOyUh94vDhN85pWkongIUhMdls89j2BtqnsFEQMyvpFoeXeqQltjdMzBwkz
RUKKnuYIGO+pwIE6UsdYEr7R4+QH/9NVBLpqjQYhb1gLxW0nDW5cgAOtQku5fi0
1T+ZwMV9ctWTuNF9Vm3aEuEDbPkfwC0xhPuHpwno2Yxvo021ZeXIYFXC6jL+E/f
iiKw2rZtZWLFJ1xSwVm1PQTm8/vb0/IBUjLs+r4qk5aiKrUyL92wRlj1G28rjd
K1yztZPSem9HvuRy1kOTEN74clnMoBzgd0H9QG31ntyivk5cwgrpm602S+UCLH7X
p031WFJmlaknSJg3yomB/jrzEzZeMWVPOUoiHxzqRA2AwqbsNOVvQts5/8p-U2AW
+fVD0xxTkijU6EiUto30aIBRvdUaEKLFWA6k+nyto2S5i1900xH5YJyHalWqtbtLA

Https

https://zimbra.free.fr/zimbra/mail#2

Calomel SSL Validation



Security : Very Strong (green 100%)
Certificate: Verified
Class : Domain Validation (DV)

URL Host : zimbra.free.fr
Common Name (CN) : *.free.fr (matched)

Perfect Forward Secrecy [PFS]: YES (20/20)

Ciphersuite : TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS Version : TLS v1.2 (10/10)
Key Exchange: ECDHE [PFS] (20/20)
Signature : RSA
Bulk Cipher : AES 128 bit (15/15)
MAC : SHA-256 AEAD GCM (15/15)

Issued to :
: SHA-256 avec chiffrement RSA 2048 bit (10/10)
Issued by : GeoTrust Inc.
: US
: SHA-256 avec chiffrement RSA 2048 bit (10/10)

Valid from : 07/06/2015 12:36:26
Valid until: 07/08/2017 16:29:34

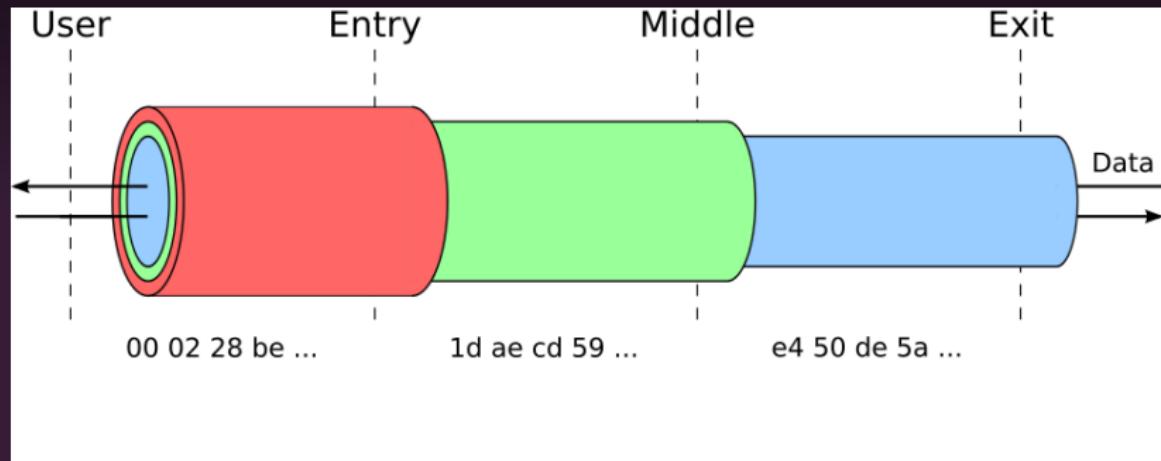
Wed Sep 23 2015 14:57:51 GMT+0200
by Calomel @ https://calomel.org

Quelques mots sur Tor ?



Attention : la présentation *complète* dure une bonne heure et demi...

Comment fonctionne Tor ?



A quoi sert TOR?

Ce que l'usage de Tor permet de faire

- d'échapper au fichage publicitaire,
- de publier des informations sous un pseudonyme,
- d'accéder à des informations en laissant moins de traces,
- de déjouer des dispositifs de filtrage (sur le réseau de son entreprise, de sa Université, en Chine ou en France...),
- de communiquer en déjouant des dispositifs de surveillances,
- de tester son pare-feu,
- ... et sûrement encore d'autres choses.

⇒ Tor dispose également d'un système de « services cachés » qui permet de fournir un service en cachant l'emplacement du serveur.

Télécharger le Tor Browser

Toutes les versions (dans différentes langues, différents OS) sont disponibles sur le site du projet :

<https://www.torproject.org/>

Rq : Il existe la possibilité de le recevoir par mail...

The screenshot shows the official Tor Project website at <https://www.torproject.org/projects/torbrowser.html.en>. The page title is "Tor Browser Bundle". The main content area features the "What is the Tor Browser?" section, which includes a purple "Tor Browser BBOM2B" logo, a "DOWNLOAD" button with a download icon, and a brief description of how the software protects users by bouncing their communications through a distributed network of relays. Below this, there's a "Installation Instructions" link for Windows, OS X, and Linux, and a "Do you like what we do? Please consider making a donation" link. At the bottom, there's a "Quick Videos on how to use the Tor Browser" section with links for "How to download and verify Tor Browser on:" (Windows, Apple OS X, Linux) and "How to use Tor Browser:" (Non-OS specific).

https://www.torproject.org/projects/torbrowser.html.en

Home About Tor Documentation Press Blog Contact

Download Volunteer Donate

HOME > PROJECTS > TORBROWSER

Software & Services: • Arm • Orion • Tails • TorTidy • Onionoo • Metrics Portal • Tor Cloud • Onionproxy • Shadow • Tor2Web

What is the Tor Browser?

TOR BROWSER BBOM2B

DOWNLOAD

The **Tor** software protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites which are blocked.

The **Tor Browser** lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained.

Installation Instructions
Windows • OS X • Linux

Do you like what we do? Please consider making a donation »

Quick Videos on how to use the Tor Browser

How to download and verify Tor Browser on:	Windows	Apple OS X	Linux
How to use Tor Browser:	Non-OS specific		

To start using Tor Browser, download the file for your preferred language. This file can be saved wherever is

Tor Browser Downloads

Lancer le Tor Browser

A propos de Tor - Navigateur Tor

A propos de Tor

Saisir un terme à rechercher ou une adresse

Le menu de l'oignon vert a maintenant un curseur de sécurité qui vous laisse ajuster votre niveau de sécurité. Découvrez le !

Ouvrir préférences de sécurité

Navigateur Tor 4.5



Félicitations !

Ce navigateur est configuré pour utiliser Tor.

Vous pouvez maintenant naviguer sur Internet de manière anonyme.

[Tester les paramètres du réseau Tor](#)

[Conseils pour rester anonyme »](#)

Que faire ensuite ?

Tor n'est PAS tout ce dont vous avez besoin pour assurer votre anonymat ! Vous devrez peut-être changer certaines de vos habitudes de navigation pour garder votre identité en sécurité.

Vous pouvez aider !

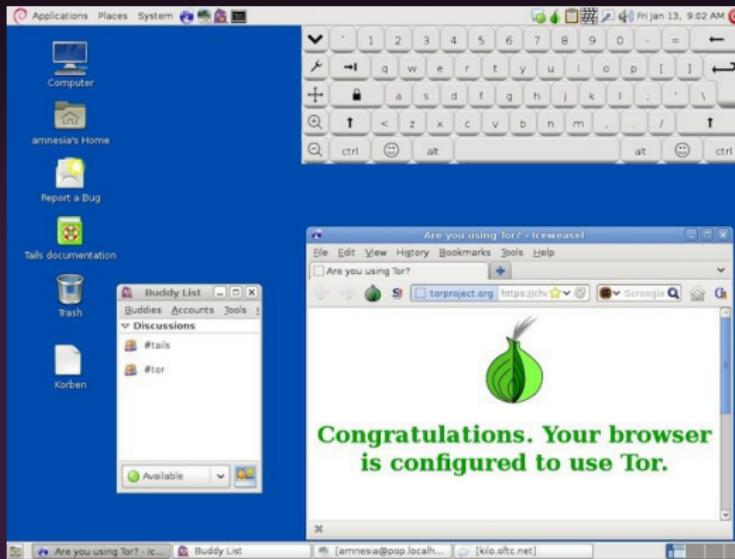
Vous pouvez aider à rendre le réseau Tor plus rapide et plus puissant de plusieurs manières :

- [Faire fonctionner un relai Tor »](#)
- [Devenir bénévole »](#)
- [Faire un don »](#)

Le projet Tor est une organisation à but non lucratif (US 501(c)(3)) dédiée à la recherche, le développement et l'éducation sur l'anonymat et la vie privée en ligne. [En savoir plus sur le projet Tor »](#)

Utiliser Tor - Tails

Tails (The Amnesic Incognito Live System) est un système d'exploitation complet basé sur Linux et Debian, en live.



<https://tails.boom.org>

Merci de votre attention.
Place aux questions.

ANNEXES

La navigation en mode privée

Quelles données ne sont pas enregistrées durant la navigation privée ?

- pages visitées ;
- saisies dans les formulaires et la barre de recherche ;
- mots de passe ;
- liste des téléchargements ;
- cookies ;
- fichiers temporaires ou tampons.

Effacer ses métadonnées

Effacer de façon sécurisé

- Pour le formatage : Shred
- Pour les métadonnées : MAT

Le logiciel MAT

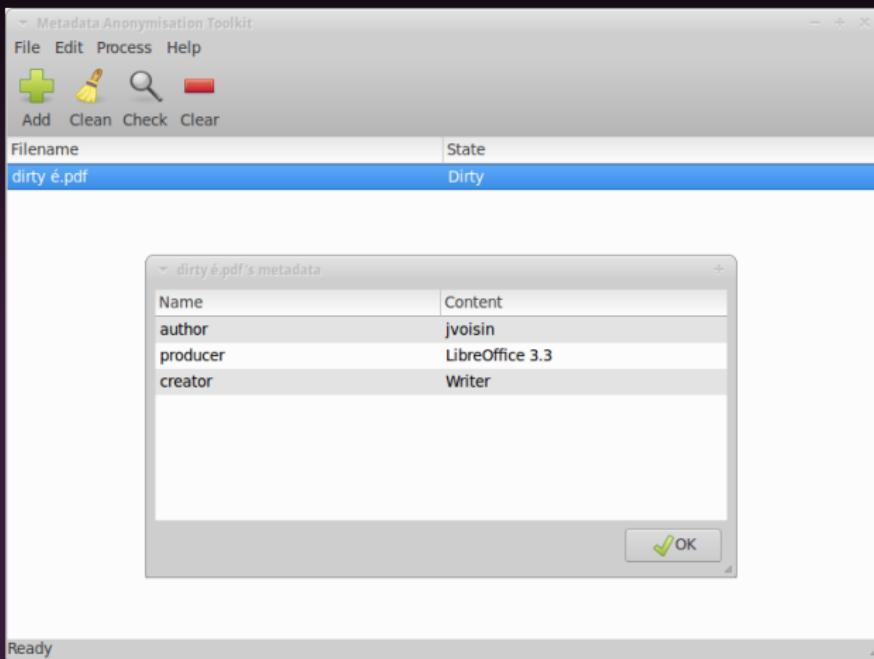
Le logiciel MAT

MAT est une boîte à outil composé d'une interface graphique, d'une version en ligne de commande et d'une bibliothèque.

MAT crée automatiquement une copie des documents originaux dans une version nettoyée (laissant intact les originaux).

MAT est fourni par défaut dans le live-cd Tails.

Le logiciel MAT



Comment vérifier rapidement la sécurité d'un site?

La check-liste

- Le site a-t-il une connexion en https? (SSL).
- Y-a-t-il intégration d'éléments extérieurs au site en lui-même?
- Le site utilise-t-il Google Analytics?
- Le site utilise-t-il Google Fonts?
- Le site utilise-t-il des régies publicitaires?
- Le site utilise-t-il Cloudflare?
- Le DNS est-il géré par Cloudflare?
- Le site présente-t-il une politique de confidentialité?
- Le site utilise-t-il les cookies?
- Le site utilise-t-il des scripts javascripts?

L'authentification forte

L'authentification forte

Différents termes, un même usage

Double authentification, Connexion en deux étapes, 2-Step Verification

Exemple avec Google

Google permet aux utilisateurs d'utiliser un processus de vérification en deux étapes.

- La première étape consiste à se connecter en utilisant le nom d'utilisateur et mot de passe. Il s'agit d'une application du facteur de connaissance.
- Au moment de la connexion Google envoie par SMS un nouveau code unique. Ce nombre doit être entré pour compléter le processus de connexion.

Il y a aussi une application à installer qui génère un nouveau code toutes les 30 secondes.

L'authentification forte

Autres services implémentant cette fonctionnalité

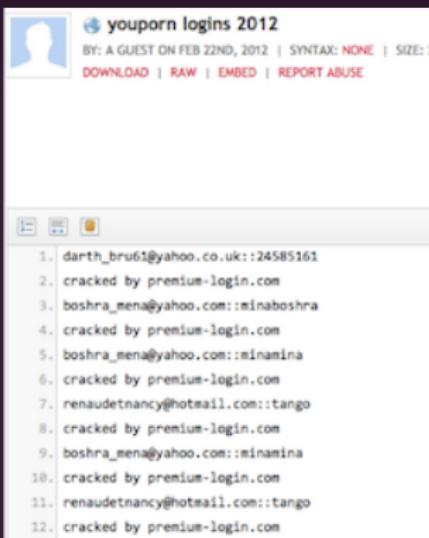
- Web : Facebook, Twitter, Linkedin, Paypal
- Banque : envoit d'un code par SMS

Des fuites de données personnelles

Le sexe par exemple. C'est perso ou pas ?

Billet Tout à cacher par Kiteoa <http://reflets.info/>

- En 2012, les identifiants et les mots de passe d'utilisateurs de Youporn ont été diffusés sur Pastebin...



The screenshot shows a Pastebin page with the title "youporn logins 2012". The page header includes a user icon, the title, and metadata: "BY: A GUEST ON FEB 22ND, 2012 | SYNTAX: NONE | SIZE: 2". Below the header are links for "DOWNLOAD", "RAW", "EMBED", and "REPORT ABUSE". The main content is a list of 12 items, each consisting of a number and a login credential:

1. darth_bru61@yahoo.co.uk::24585161
2. cracked by premium-login.com
3. boshra_mena@yahoo.com::minaboshra
4. cracked by premium-login.com
5. boshra_mena@yahoo.com::minamina
6. cracked by premium-login.com
7. renaudetnancy@hotmail.com::tango
8. cracked by premium-login.com
9. boshra_mena@yahoo.com::minamina
10. cracked by premium-login.com
11. renaudetnancy@hotmail.com::tango
12. cracked by premium-login.com

Le sexe par exemple. C'est perso ou pas ?

Billet Tout à cacher par Kiteoa <http://reflets.info/>

- Une boutique en ligne de type sexshop s'est fait piratée... Chacun a le droit de garder pour lui le fait qu'il achète (ou pas) des surtout si « chacun » a utilisé son mail professionnel pour passer commande...

```
$ cat mail.txt |  
...@culture.gouv.fr;Sarah;Fau  
...@budget.finances.gouv.  
...@jeunesse-sports.gouv.  
...@sante.gouv.fr;;Vrai  
...@equipement.gouv.fr;Aude;  
...@interieur.gouv.fr;Oli
```