

# Sécurité et vie privée

## Démystifions les dangers d'Internet !

Genma

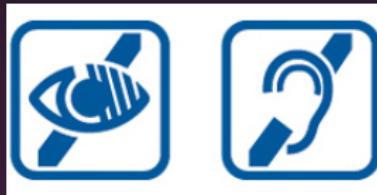
October 17, 2016



# Accessibilité

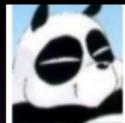
## Visuelle

- Est-ce que tout le monde arrive à lire la présentation ?
- Elle est disponible en ligne, pas la peine de prendre de notes :-)



## Auditive

- Je parle vite. Très vite.
- Merci de me faire signe pour me demander de ralentir, d'articuler.



# À propos de moi

## Où me trouver sur Internet?

- Le Blog de Genma :  
<https://blog.genma.fr>
- Twitter :  
<https://twitter.com/genma>



**Rencontre avec Genma IRL.**

publié le 5 août 2013 par Genma

Si tu ça un fétiche régulier de ce blog, que tu souhaitais me voir autour d'un verre, pour manger dans un resto et/ou tout simplement discuter, contacte moi que l'on se fixe un rendez-vous. En effet, je serai disponible du dimanche 11 août au mardi 20 août, en fin de journée ou le soir, à l'endroit que tu souhaiteras, sur Paris, France. Si tu es partant, fais signe... A la suite de cette rencontre, je pourrais faire (ou non), si tu ca d'accord, un petit moment à rendre sur mon blog, ainsi que quelques (...).

**POUR LIRE LA SUITE...**

6

---

**Lifehacking - L'importance du matériel**

publié le 2 août 2013 par Genma

Un bon ordi doit avoir de bons outils pour faire du bon travail. Le meilleur musicien ne sera pas aussi 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 qui compte.

En fait si. Pendant deux ans, sur ma mission précédente, j'avais pour travailler du bêta-ron. Un écran 22" et un clavier 19" (celui du portable). Un surdoué de l'autre. Avec ma nouvelle maison, je suis passé sur un unique écran de 17", avec un PC plus lent (je (...)).

**POUR LIRE LA SUITE... TAGS : Lifehacking**

6

Syndica

shaa

Plaistr

Twitter

Google+

RSS

Picssw

Feedburner

Data de mis

Le 5 août

rechercher

Google Recherche

OK

Catalog

Actualités GE

semaine

Blog : tout

# De quoi allons-nous parler?

Deux parties :

- Hygiène numérique et des règles de bases
- Vie privée sur Internet & données personnelles

# Un peu d'hygiène numérique



# L'hygiène numérique?

## Une définition?

L'hygiène est un ensemble de mesures destinées à prévenir les infections et l'apparition de maladies infectieuses.

L'hygiène numérique, ce sont des règles destinées à mieux utiliser son ordinateur, en sécurité, de façon simple.

*L'hygiène numérique c'est comment éviter la gastro-informatique.*

# Un exemple

## On me vole mon PC

- Quelles sont les données que je perds ? Amène la notion de *sauvegarde*.
- Quelles sont les données que l'on trouve ? Amène la notion de *chiffrement, de coffre-fort numérique*.



# Sauvegarde simple et efficace

## Le disque dur externe

- Méthode simple : copier-coller.
- Méthode plus avancé : on "synchronise".
- On le dépose chez un ami, un voisin, un parent (pour éviter le vol, l'incendie...)

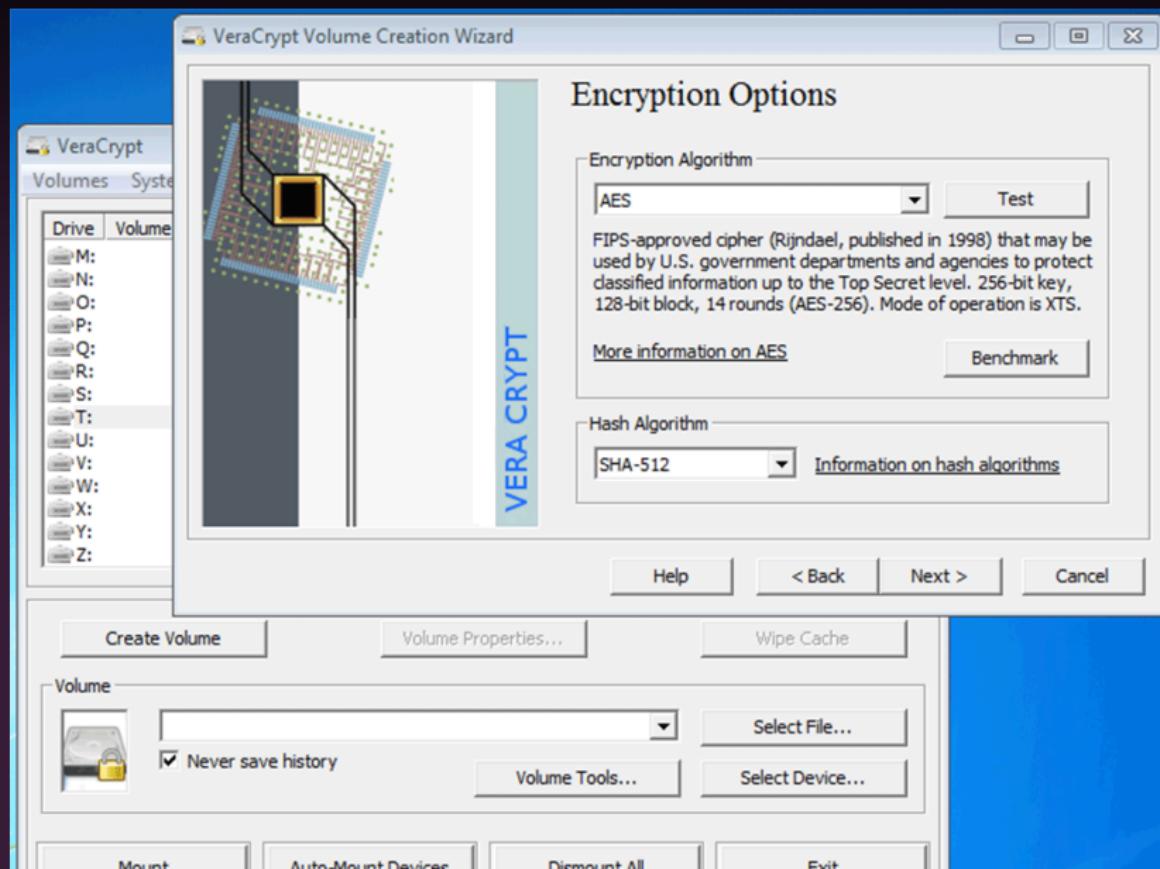
Petit plus : chiffrer le disque pour plus de confidentialité.



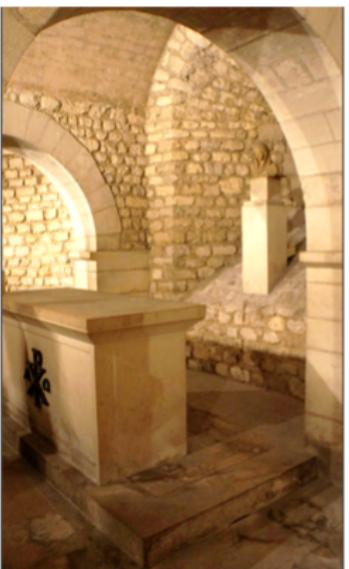
# Coffre-fort numérique ? Veracrypt



# Coffre-fort numérique ? Veracrypt



Crypté ? Cryptage ?



**Mes données  
sont protégées,  
je les ai  
cryptées  
*chiffrées.***



# Les mots de passe



# Les mots de passe

## Règles

- Plus c'est long, plus c'est bon
- Ne pas avoir le même mot de passe pour deux comptes en ligne.
- Passer à des *phrases de passe* (technique des dés...)

## Trop de mot de passe à retenir?

Il y a le logiciel KeepassX.

# KeePassX, le coffre-fort numérique des mots de passe

The screenshot shows the KeePassX application interface. At the top, there's a toolbar with icons for file operations like Open, Save, Print, and a search bar. Below the toolbar is a title bar showing the path /Users/robbrown/a.kdb – KeePassX.

The left side features a tree view titled "Groups" containing the following categories:

- Domain Registrars
- Affiliate Accounts
- Outsourcing We...
- Programming R...
- Misc Websites
- Personal Websites
- Work Websites
- Work VPNs
- Proxies
- Routers
- Server Clusters
  - 1-1
  - 1-2
  - 2-1
  - 2-2
- Household

The right side displays a table of password entries:

Title	Username	URL	Password	Comment
1&1 Dom...	***...	http://www.land1.c...	**...	
Enom	***...	http://www.enom.c...	**...	
Gandi	***...	http://www.gandi.n...	**...	
Godaddy	***...	http://www.godadd...	**...	
Name.com	***...	http://www.name.c...	**...	
NameCheap	***...	http://www.namech...	**...	
Netfirms	***...	http://www.netfirm...	**...	
Network S...	***...	http://www.network...	**...	

# Les mots de passe

## Les sites permettant de tester ses mots de passes?

- Ils sont la meilleure façon de constituer une base de données de mots de passe.
- Ne pas tester son vrai mot de passe mais un mot de passe du même type/de la même forme.
- Les mots de passe sont personnels

## Parents - enfants

Tant qu'on est mineur on doit les donner à ses parents. Les parents qui sont des gens bien et responsables, ne sont pas là pour les utiliser pour espionner leurs enfants mais seulement au cas où.

# Gestion des comptes

## Des comptes pour des usages différents

- Créer un compte utilisateur et un compte administrateur.
- Au quotidien, utiliser le compte utilisateur.
- Le compte administrateur porte bien son nom, il ne doit servir qu'aux tâches d'administration (installation des logiciels...)

Quand l'ordinateur pose une question "Je dois lancer ce programme", réfléchir. Ne pas dire oui tout de suite.

# Mises à jour de sécurité

## FAIRE LES MISES A JOUR

- Avoir un système à jour.
- Avoir des logiciels à jour.
- Avoir un antivirus à jour.

## Les logiciels ont des bugs

- Un bug peut-être utilisé par un virus...
- Mettre à jour, c'est corriger les bugs, donc se protéger.

# Mises à jour de sécurité

Control Panel Home

Check for updates

**Change settings**

View update history

Restore hidden updates

Updates: frequently asked questions

Control Panel > Control Panel > System and Security > Windows Update

Search Control Pa... ?

## Windows Update

 Download and install updates for your computer

14 important updates are available

1 optional update is available

**13 important updates selected, 55.1 MB**

**Install updates**

Most recent check for updates: Today at 8:05 AM

Updates were installed: 5/25/2011 at 7:39 PM. [View update history](#)

You receive updates: For Windows and other products from Microsoft Update

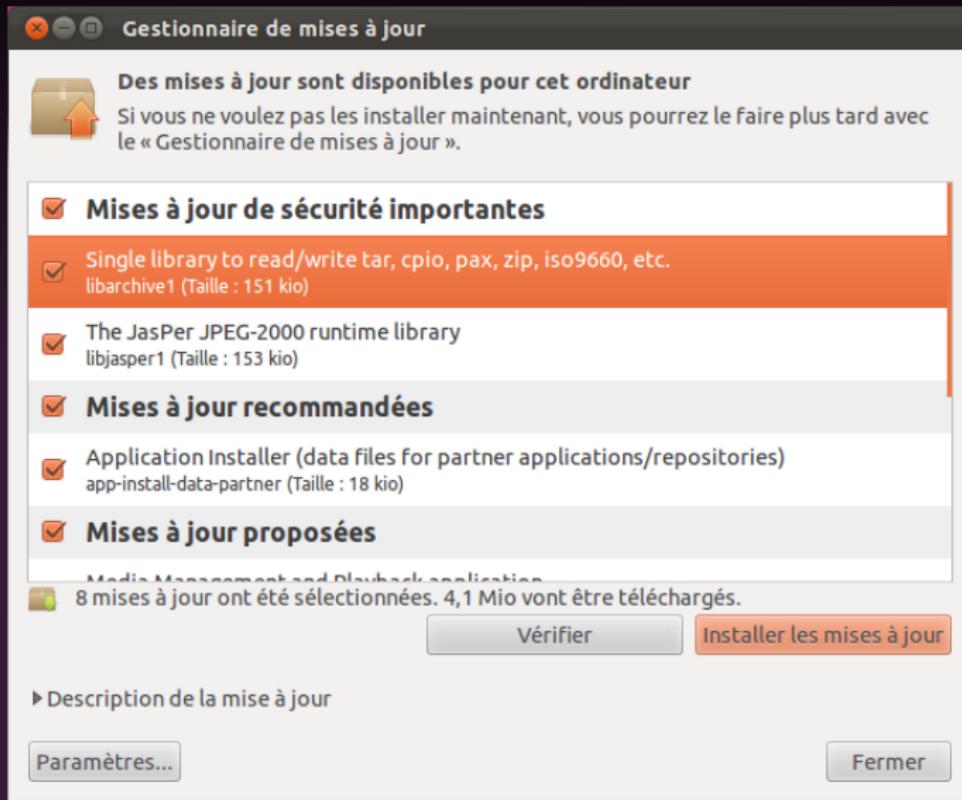
Find out more about free software from Microsoft Update. [Click here for details.](#)

See also

Installed Updates

 Windows Anytime Upgrade

# Mises à jour de sécurité



# Installation de logiciels

## Logiciels payants - propriétaires

- Pas de logiciels crackés
- Pas de téléchargement de logiciels depuis un autre site que le site officiel. On oublie les sites 01Net, Télécharger.com qui remplacent le navigateur par Chrome...
- Que les logiciels dont on a besoin (pas de démos, de logiciels marrants...)

## Logiciels libres

- Préférer le logiciel libre - open source.
- Passer par l'annuaire de Framasoft.

# Le copain qui s'y connaît

## Attention

- Ne pas le laisser installer les logiciels crackés.
- Chercher à comprendre ce qu'il fait, lui demander.
- S'il n'est pas capable d'expliquer, se méfier. Voir refuser.

## PC = Personal Computer

- Ne pas faire confiance. Il ne faut pas prêter sa machine sans voir ce que fait l'individu à qui vous l'avez confiée.
- Il faut prévoir une session invitée.
- Il est si facile d'installer un virus sur un PC... Méfiez-vous de ce que l'on fait sur votre PC.

# Résumé

## Bilan

- Vous voulez éviter le gros de la contamination virale : GNU/Linux.
- Evitez les sites de Warez, de porno, les installations de logiciels piochés à gauche et à droite sur la toile, les clés USB.
- De façon générale, lisez, apprenez, documentez-vous, ayez une utilisation rationnelle de votre ordinateur.

En appliquant, ces règles, on a tout de suite beaucoup moins de soucis avec son PC.

# Hygiène numérique & Internet

Internet, quels principes

# Internet, un réseau de réseau

- Internet c'est un réseau de réseau d'ordinateurs connectés entre eux.
- Il y a les serveurs, des gros ordinateurs, sur lesquels il y a des sites Internet.
- Il y a des routeurs, qui servent à transmettre les colis que l'on appelle "des paquets".
- Il y a la Box Internet qui est un point d'entrée de sortie sur Internet
- Et enfin il y a notre ordinateur/tablette/smartphone...

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

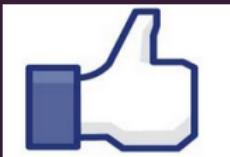
Les données qui sont prises à  
notre insu...

Comment est-on suivi à la trace  
sur Internet?

# 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...



# Pour le voir, l'extension Lightbeam

Lightbeam

resource://jid1-f9uj2thwoam5qq-at-jetpack/lightbeam/data/index.html

DATA GATHERED SINCE OCT 23, 2015 YOU HAVE VISITED 19 SITES YOU HAVE CONNECTED WITH 293 THIRD PARTY SITES

TRACKING PROTECTION OFF

LAST 10 SITES

GRAPH VIEW

zDnet.fr

FIRST ACCESS Fri, Oct 23, 2015 3:14PM  
LAST ACCESS Fri, Oct 23, 2015 3:15PM

Block Site

Server Location

France

Connected to **56 sites** since first access.

Visited Sites Watched Sites

Third Party Sites Blocked Sites

Connections Cookies

The screenshot shows the Lightbeam extension interface within a Firefox browser window. The main area displays a network graph titled 'Last 10 Sites' with various nodes representing websites like 'zDnet.fr', 'google.fr', and 'ajax.googleapis.com'. Nodes are represented by icons and letters (e.g., a red square with 'zD', a white circle with 'g', a blue triangle with 'a'). Lines connect nodes to show their relationships. On the left, a sidebar has 'Graph' selected under 'VISUALIZATION'. Below it are 'Save Data' and 'Reset Data' buttons, and a link to 'Give Us Feedback'. The right side shows detailed information for 'zDnet.fr', including its first and last access times, a 'Block Site' button, its server location in France, and a world map indicating its origin. A summary at the bottom states 'Connected to 56 sites since first access.' and lists some of the tracked sites.

# Cloud - l'informatique dans les nuages

## Définition du cloud

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



**There is no cloud**

it's just someone else's computer

# LES GAFAMs



# Les GAFAM

GAFAM : Google, Apple, Facebook, Amazon, Microsoft

- Concentration des acteurs d'Internet autour de silos ;
- Une centralisation nuisible (frein à l'innovation) ;
- Les utilisateurs de ces services ne contrôlent plus leur vie numérique.

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

# Hygiène numérique & Internet

# Choisir le bon navigateur



# La navigation en mode privé 1/2

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.

# La navigation en mode privé 2/2

Fichier Édition Affichage Historique Marque-pages Outils ?

Navigation privée

Saisir un terme à rechercher ou une adre. Rechercher

Nouvelle fenêtre de navigation privée

Non conservé	Conservé
✓ L'historique	⚠ Les téléchargements
✓ Les recherches	⚠ Les marque-pages
✓ Les cookies	
✓ Les fichiers temporaires	

Veuillez noter que votre fournisseur d'accès à Internet ou votre employeur peuvent toujours connaître les pages que vous visitez.

[En savoir plus...](#)

Protection contre le pistage

**ACTIVÉE**



Les fenêtres privées bloquent désormais les éléments qui peuvent pister votre navigation

# Installer des extensions

S'inscrire ou Se connecter Autres applications ▾ mozilla

## MODULES

EXTENSIONS | THÈMES | COLLECTIONS | PLUS ...

recherche de modules ➔

**EXPLORER**

- En vedette
- Les plus populaires
- Les mieux notés

**CATÉGORIES**

- Alertes et mises à jour
- Apparence
- Développement web
- Flux, nouvelles et blogs
- Gestion des téléchargeme...
- Jeux & divertissements
- Marque-pages
- Onglets
- Outils de recherche
- Outils linguistiques
- Photos, musique et vidéos
- Shopping

EN VEDETTE

Extensions > Sécurité et vie privée

### Sécurité et vie privée

**Ghostery** **WOT - Naviguez sans ris...** **TinyURL Generator**

**Les plus populaires** Tout voir ▾

 <b>Adblock Plus</b> Sécurité et vie privée ★★★★★ (4 978)	 <b>No Script</b> Sécurité et vie privée ★★★★★ (1 504)	 <b>Ghostery</b> Sécurité et vie privée ★★★★★ (1 224)
 <b>Adblock Plus Pop-up ...</b> Sécurité et vie privée ★★★★★ (182)	 <b>WOT - Naviguez sans ...</b> Outils de recherche ★★★★★ (1 645)	 <b>LastPass Password ...</b> Social et communication ★★★★★ (1 245)

# Ublock Origins - Bloquer les publicités

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

Fichier Édition Affichage Historique Marque-pages Outils ?

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

www.01net.com

W Wikipedia (fr)

01net nos newsletters nos magazines

01net Utilisez 01net pour 2,45 €/m<sup>2</sup> seulement

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

**Olnet** Rechercher un logiciel OK

**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.

**Apple renouvelle sa gamme iPad et met son**

**Harman Kardon Onyx : un son et un design au top**

**La CHAÎNE TECHNO** 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... 23/10/2013 à 07:00

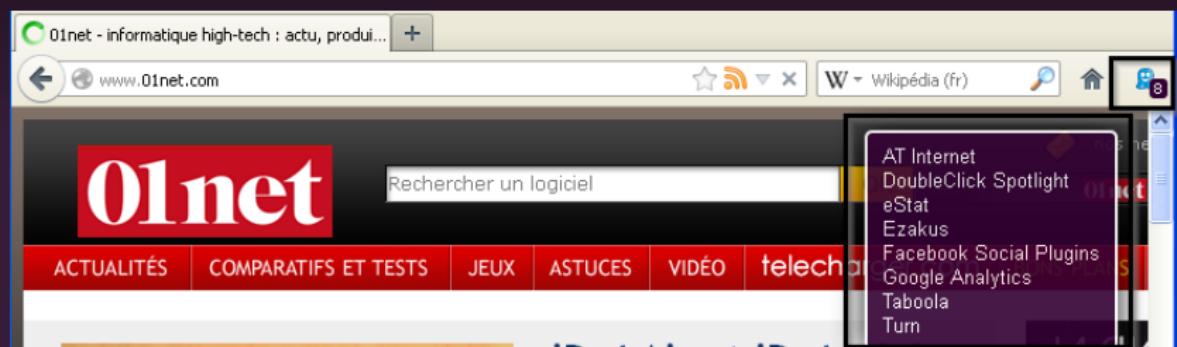
Découvrez la Nvidia Shield, une console "concept" sous Android qui... 21/10/2013 à 07:00 > Toutes les vidéos

**TOP TESTS**

01 | Samsung Galaxy Note 3, le champion incontesté des smartphones

# Ghostery, Privacy Badger, Noscript...

Bloquer tous les trackers associés au site.



# Changer de moteur de recherche

Don't be evil

Duckduckgo - Google tracks you. We don't.

<https://duckduckgo.com>



DuckDuckGo

Le blog de Genma



Saviez-vous que vous pouvez [personnaliser DuckDuckGo](#) ?

• • • •



Faire de DuckDuckGo votre moteur de recherche par défaut



Framabee <https://framabee.org>

ou TontonRoger <https://tontonroger.org/>

The screenshot shows the Framabee search interface. At the top, there's a header with the Framasoft logo and navigation icons. Below it is the search bar with the Framabee logo and a gear icon. The search bar contains the text "Le blog de Genma". To the right of the search bar are a magnifying glass icon and a close button. The main content area features a large question mark icon inside a dark circle. Below this icon, text explains what Framabee is and its privacy policy.

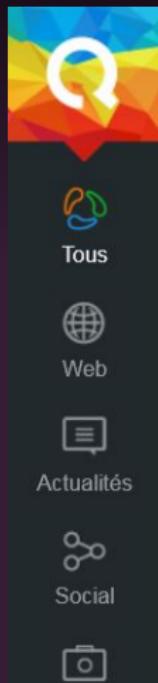
## Spécificité

Framabee est un métamoteur de recherche regroupant les résultats d'autres moteurs de recherche mais sans conserver d'informations sur les utilisateurs.

Framabee ne vous trace pas, ne partage aucune donnée avec un tiers et ne peut pas être utilisé pour vous compromettre.

# Qwant

<https://qwant.com>



Connexion

FR



**Qwant®**  
Beta

Actualités

Le blog de Genma



# Changer de Cloud



# Framasoft et tous ses outils de Degooglisons

## Dégooglisons Internet

Une initiative du réseau **Framasoft** en faveur d'un internet libre, décentralisé, éthique et solidaire

Cliquez sur la carte pour découvrir les alternatives...

[Soutenir ce projet](#)

### Liste des services

Village libriste

#### Village libriste

Au milieu des multinationales tentaculaires, quelques organisations non-lucratives continuent de lutter activement pour un Web ouvert et respectueux des internautes.

En plus de **Framasoft**, association loi 1901 qui mène la présente campagne, nous pouvons citer [l'April](#), [la Quadrature du Net](#) ou encore [l'Aful](#). Ces associations vivent de vos dons, n'oubliez pas de les soutenir !



[Les enjeux](#)

[Les dangers](#)

[Nos propositions](#)

[Concrètement](#)

# Cozycloud



# Owncloud /NextCloud

The screenshot shows the Owncloud/NextCloud web interface. On the left, a sidebar lists various categories: Fichiers, Musique, Contacts, Calendrier, Tâches, Images, Favoris, and Impress. The main area displays a list of files and folders. At the top of the list is a new folder named "Nom". Below it are several demo files: "Music" folder, "Photos" folder, "Demo Code - C++ .cc", "Demo Code - PHP .php", "Demo Code - Python .py", "Demo Image - ccc .jpg", "Demo Image - Laser Towards Milky Ways Centre .jpg", "Demo Image - Northern Lights .jpg", "Demo Movie MOV - Big Bug Bunny Trailer .mov", "Demo Movie OGG - Big Bug Bunny Trailer .ogg", "Demo MP3 - E.J. - Blick Zurück .mp3", "Demo PDF - Alice in Wonderland .pdf", "Demo Presentation - Bored .impress", and "Demo Textfile - License .txt". To the right of the file list are columns for Taille (Size) and Modifié (Last modified). Below the file list is a "Partager avec" (Share with) panel. It contains several checkboxes: "Partager via lien" (Share via link) which is checked, "Protéger par un mot de passe" (Protect with password), and "Spécifier la date d'expiration" (Specify expiration date). The URL "http://demo.owncloud.org/public.php" is listed under the share link. A "Send" button is at the bottom right of the panel.

	Taille	Modifié
Nom	70.3	il y a 6 minutes
Music	< 0.1	il y a 6 minutes
Photos	< 0.1	il y a 6 minutes
Demo Code - C++ .cc	< 0.1	il y a 6 minutes
Demo Code - PHP .php	< 0.1	il y a 6 minutes
Demo Code - Python .py	< 0.1	il y a 6 minutes
Demo Image - ccc .jpg	0.2	il y a 6 minutes
Demo Image - Laser Towards Milky Ways Centre .jpg	0.3	il y a 6 minutes
Demo Image - Northern Lights .jpg	0.2	il y a 6 minutes
Demo Movie MOV - Big Bug Bunny Trailer .mov		
Demo Movie OGG - Big Bug Bunny Trailer .ogg		
Demo MP3 - E.J. - Blick Zurück .mp3		
Demo PDF - Alice in Wonderland .pdf		
Demo Presentation - Bored .impress		
Demo Textfile - License .txt		

Partager avec

Partager via lien  
http://demo.owncloud.org/public.php

Protéger par un mot de passe

Email link to person

Spécifier la date d'expiration

Send

# La brique Internet

<http://labriqueinter.net>



# Yunohost



**genma**

gemma kun  
genma@genma.org

⚡ Décon...

**Ag**

AgenDAV

**Ba**

Baikal

**Cu**

Custom Webapp

**Do**

Dokuwiki

**Ka**

Kanboard

**Ow**

OwnCloud

**SP**

SPIP

**So**

Sonerezh

**Ti**

Tiny Tiny RSS

**Wa**

Wallabag

**Ze**

Zerbin

**ph**

phpMyAdmin

Pour vous aider,

Le monde associatif

# Sur Paris - Parinux

## Premier Samedi du Libre (PSL)

Chaque premier samedi de chaque mois, les bénévoles des associations du Libre vous accueillent au Carrefour Numérique de la Cité des sciences et de l'industrie (CSI) pour une install party.

<http://premier-samedi.org/>



# Ubuntu Party

Ubuntu-fr

Ubuntu Party <http://www.ubuntu-paris.org/>



# Agenda du libre

<http://www.agendadulibre.org/>



## L'Agenda du Libre

Les événements du Libre en France

Île-de-France

Trouve ton Orga! 

<< Octobre 2015 >>

Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche
28	29	30 Paris: Kernel Recipes	1 Paris: Kernel Recipes <b>Paris:</b> Soirée de contribution au libre	2 Paris: Kernel Recipes	3 <b>Argenteuil:</b> Atelier sur GSN3, Graphic Simulator Network	4
5	6	7	8 <b>Paris:</b> Soirée de contribution au libre <b>Paris:</b> Paris Embedded Meetup #7	9	10	11
12	13	14	15	16	17 <b>Gonesse:</b> Install party Linux <b>Versailles:</b> Café vie privée - Chiffrofête	18
19	20	21	22 <b>Paris:</b> Soirée de Contribution au Libre	23	24	25

Café vie privée, chiffrofête,  
cryptoparty



Café *vie privée*

Merci de votre attention  
Place aux questions.





Me contacter?

Le Blog de Genma

<https://blog.genma.fr>

Twitter : @genma

# ANNEXES

# Règles de sécurité supplémentaires

# 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 : envoi d'un code par SMS

# 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 javascript ?

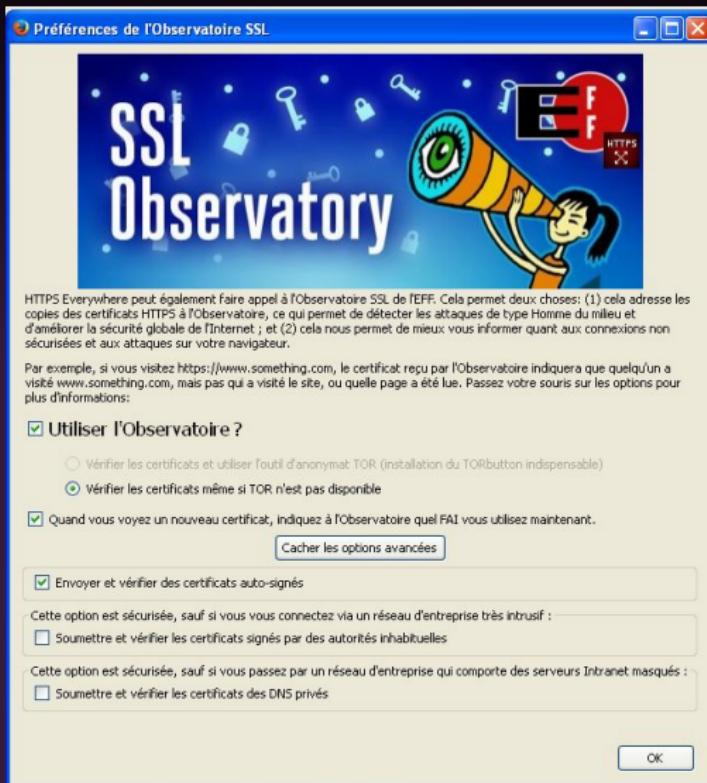
httpS

# HTTPSEverywhere

Force le passage en https quand celui-ci est proposé par le site.

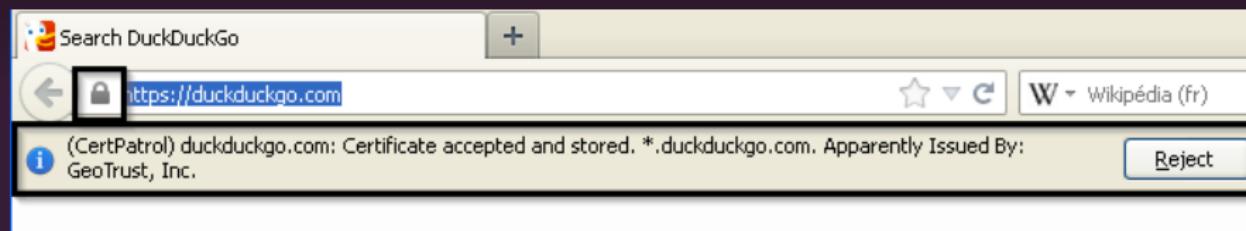


# HTTPSEverywhere



# Certificate Patrol

Permet de valider les certificats d'un site (lié à https).



# Certificate Patrol

**Certificate Patrol**

**Certificate exchanged. Reason to be careful!** (pbs.twimg.com)

**Alert:** Hostname has changed. Take a look if that's okay.

**Caution:** Certification Authority has changed.

**Info:** This certificate will expire soon. It is normal to replace it now.

Old Certification Hierarchy:  
[View Old Certificate](#)

- DigiCert High Assurance EV Root CA
- DigiCert High Assurance CA-3
- \*.twimg.com

New Certification Hierarchy:  
[View New Certificate](#)

- VeriSign Class 3 Public Primary Certification Authority - G5
- VeriSign Class 3 Secure Server CA - G3
- si0.twimg.com

Issued To:

Common Name (CN):  
- \*.twimg.com  
+ si0.twimg.com

Organization (O):  
Organizational Unit (OU):

MDS Fingerprint:  
- D2:CA:A0:13:55:96:A4:4E:A6:59:2A:C2:B8:D3:AF:C2  
+ C9:13:83:7C:64:AD:82:99:DF:6B:73:B2:E7:C6:D7:A8  
- 22:7B:7E:23:04:CE:DF:2C:68:21:08:35:59:67:3B:CC:58:49:46:53  
+ 1E:A8:A4:26:C9:BC:CC:E1:70:48:E0:77:A9:43:CC:EC:79:F4:AF:50

SHA1 Fingerprint:

Validity:

Issued On:  
- 2013-03-27 01:00:00 (301 days ago)  
+ 2013-05-01 02:00:00 (266 days ago)

Expires On:  
- 2014-04-01 14:00:00 (69 days ahead)  
+ 2014-06-11 01:59:59 (140 days ahead)

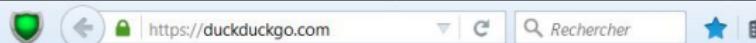
Stored Since:  
2013-10-23 16:14:16 (91 days ago)

Apparently Issued By:

Too many pop-ups? Try checking authority only for this domain

**Accept** **Ignore this website** **Reject**

# Calomel SSL



## Calomel SSL Validation

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

URL Host : duckduckgo.com  
Common Name (CN) : \*.duckduckgo.com (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 : Duck Duck Go, Inc.  
: Paoli Pennsylvania US  
: SHA-256 avec chiffrement RSA 2048 bit (10/10)  
Issued by : DigiCert Inc  
: US  
: SHA-256 avec chiffrement RSA 2048 bit (10/10)

Valid from : 06/06/2015 02:00:00  
Valid until: 22/06/2016 14:00:00

Wed Oct 07 2015 17:38:21 GMT+0200  
by Calomel @ <https://calomel.org>

# Utilisation d'Internet depuis un lieu public

# Utilisation d'un PC d'un Cybercafé?

## Pour le surf Internet

- Eviter les sites sur lesquels on sait des données personnelles : webmail, réseaux sociaux
- Vérifier la version du navigateur
- Ne pas mémoriser vos informations confidentielles
- Penser à fermer votre session
- Effacer vos traces de navigation

Ne pas brancher de clef USB (virus), ne pas récupérer de documents.  
Idéalement ? Un navigateur en mode portable, depuis une clef USB  
Encore mieux : rebooter sur un live-usb/cd

# Wi-Fi public?

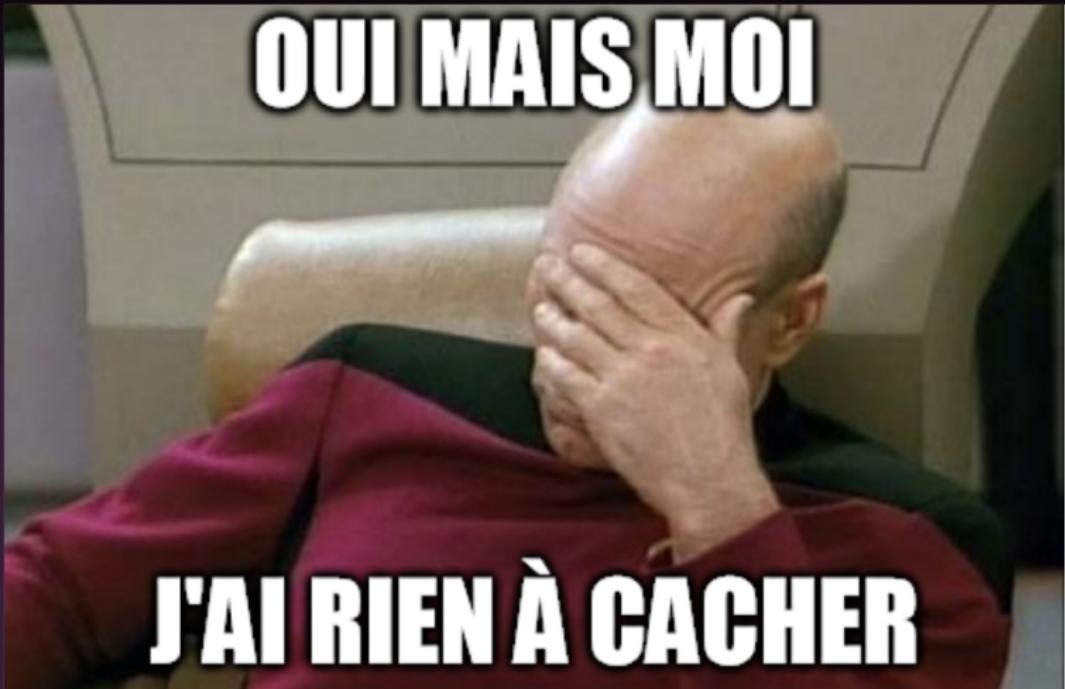
Ne pas avoir confiance. Utiliser sa propre machine.

## Attention à la sécurisation

- Au minimum : connexion HTTPS
- Mieux, passer par un VPN

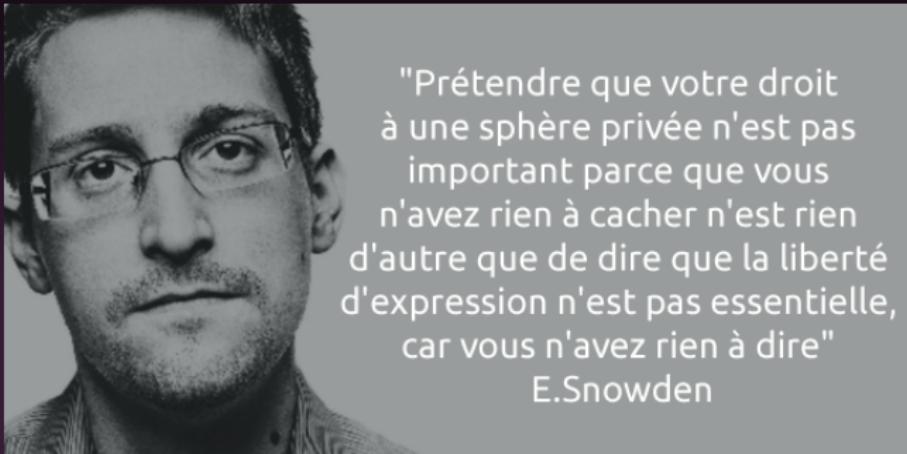
# Internet & Surveillance

**OUI MAIS MOI**



**J'AI RIEN À CACHER**

# L'espionnage 1/2



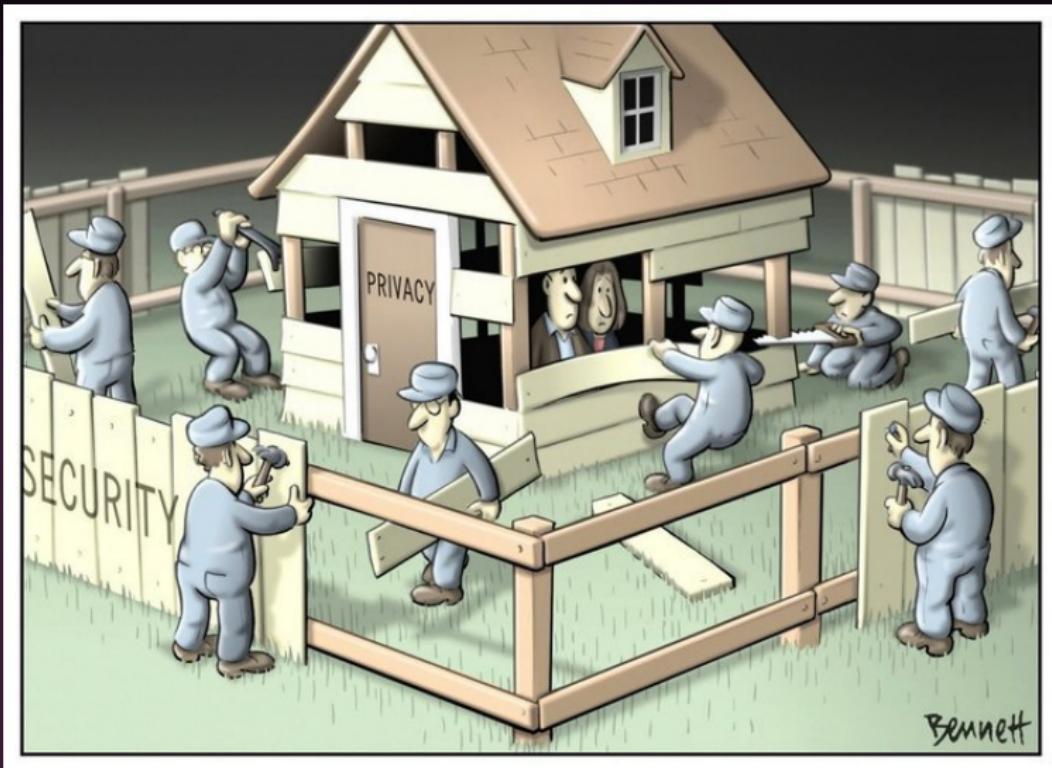
- Snowden et ses révélations (NSA)
- La loi Renseignement en France...

# L'espionnage 2/2

- Notre voisin
- Notre "ex"
- Notre collègue de boulot



# La différence entre la vie privée et la sécurité en une image



# Différents modèles de menace

## Répondre aux questions

Pour se faire un avis <http://jenairienacacher.fr/>

- Quelles sont les données et informations que j'estime personnelles - confidentielles?
- Qu'est ce que je suis prêt-e à apprendre et à faire pour les protéger?
- Usage d'un pseudonyme...

