

# Petit guide d'hygiène numérique

Genma

October 7, 2015



This work is licensed under the *Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License*.

# L'hygiène numérique?

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

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

# Quelques règles

# Les règles de sécurité



- Ne pas exposer l'animal à la lumière — et plus spécialement à celle du soleil qui le tuerait,
- Ne pas le mouiller,
- Et surtout, quoi qu'il arrive, ne jamais lui donner à manger après minuit.

Plus sérieusement

# Règle 0 - Mises à jour de sécurité

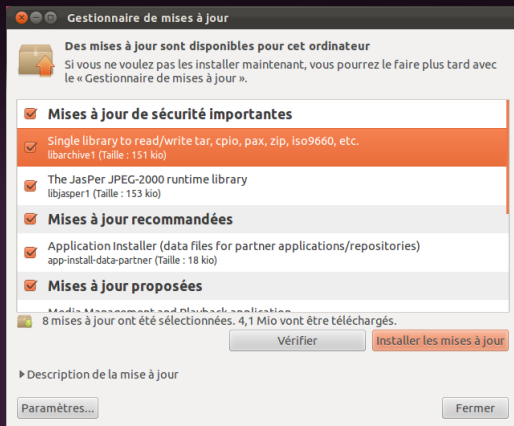
## FAIRE LES MISES A JOUR

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

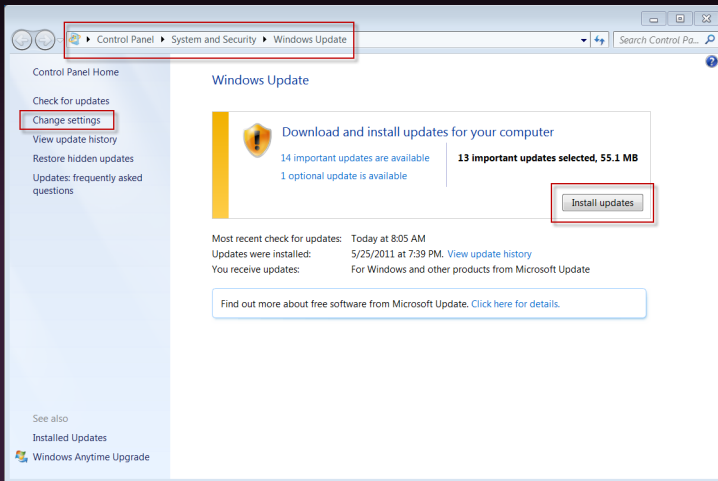
## Les logiciels ont des bugs

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

# Règle 0 - Mises à jour de sécurité



# Règle 0 - Mises à jour de sécurité





# Règle 1 - 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.

# Règle 2 - Mots de passe

## Règles

- Plus c'est long, plus c'est bon
- Ne pas avoir le même mot de passe pour deux comptes en lignes.

## Mot de passe oublié?

Pour tester la sécurité d'un site web, on clique sur le lien "mot de passe oublié".

- Si le mot de passe est renvoyé dans le mail, ce n'est pas bon. Le mot de passe est stocké "clair".

## Trop de mot de passe à retenir?

Il y a le logiciel Keepass. <http://www.Keepass.info>

## Règle 2 - 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.

## Règle 3 - Les mails

### Phishing - Hameçonnage

- Ne JAMAIS envoyer d'argent. Même à un ami.
- Etes vous sûr que c'est bien votre banque?

**Toujours lire et réfléchir avant de cliquer.**

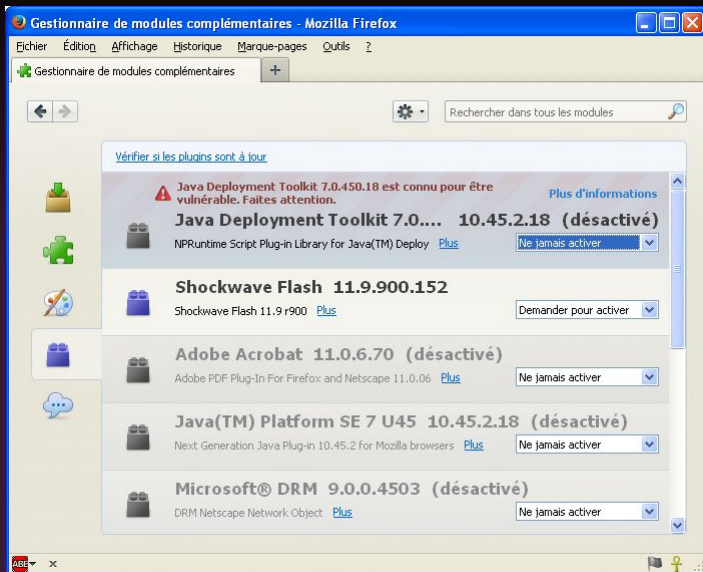
# Règle 4 - Le navigateur

## Utiliser Firefox

- Firefox doit être à jour.
- Les plugins (Flash, Java) doivent être à jour.
- Les extensions doivent être à jour.
- Supprimer les plugins inutiles.



# Règle 5 - Les plugins



# Règle 6 - 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
- 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.

# Règle 7 - 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. Voire refuser.

## PC = Personal Computer

- Ne pas faire confiance. Il ne faut prêter sa machine sans voir ce que fait l'individu à qui vous l'avez confié.
- 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.



# Règle 8 - Résumé

## Bilan

- Vous voulez éviter le gros de la contamination virale : 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.
- Enfin le cas échéant, quelques outils comme Malwarebytes anti-malware ou Adwcleaner sont efficaces pour vérifier si la machine est saine.

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

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

# Les sauvegardes



Mon PC ne marche plus, on  
me le vole... Quelles sont les  
données que je perds? Quelle  
importance ont ces données  
pour moi?



# Notre vie numérique

De plus en plus de données sont sur nos ordinateurs

- Les photos de vacances,
- Les factures...

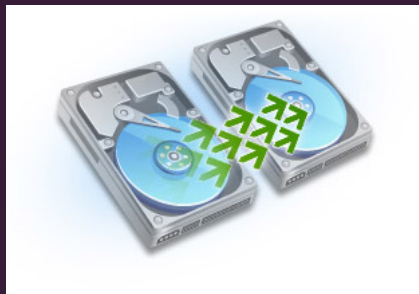
Comment les préserver?

# 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.



# Sauvegarder dans le cloud?

## Pratique mais...

- Quid de la pérennité des données?
- De la confidentialité des données?





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

# La Navigation privée

Naviguer sur Internet sans conserver d'informations sur les sites que vous visitez. Avertissement : La navigation privée n'a pas pour effet de vous rendre anonyme sur Internet. Votre fournisseur d'accès Internet, votre employeur ou les sites eux-mêmes peuvent toujours pister les pages que vous visitez.

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

Changer de moteur de  
recherche

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 par Framasoft

<https://framabee.org>



The screenshot shows the web interface of Framabee. At the top left is the Framasoft logo. In the center is the Framabee logo, which includes a stylized bee icon. To the right of the logo is a gear icon for settings. Below the logo is a search bar containing the text "Le blog de Genma". To the right of the search bar are search and close icons. The main content area has the heading "Spécificité" followed by a large question mark icon. Below this, there are two paragraphs of text explaining the service's privacy policy.

**Framasoft**

**Framabee**

Le blog de Genma

## 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>





# Annexes

# 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