# Les 11 commandements de l'informatique



## Des sauvegardes régulières, tu feras !

Le premier commandement vous ordonne de **sauvegarder régulièrement vos données sur des supports que vous pourrez ranger à l'extérieur de l'ordinateur** (disques dur amovibles, clé usb). La sauvegarde est plus importante que tout le reste ! Comparez le temps passé à faire vos sauvegardes aux années de données perdues et, probablement, impossibles à reconstituer, et faites votre choix.

## La mise à jour, tu pratiqueras !

Appliquer régulièrement les mises à jour à votre système d'exploitation et à vos applications, ce qui ne se limite pas à faire un Windows Update !
Il n'existe pas de programme 100% sans erreur. Les mises à jour réparent non seulement des erreurs de fonctionnement des programmes, ou ajoutent de nouvelles fonctionnalités, mais corrigent également des failles de sécurité. Allez sur les sites des éditeurs de vos logiciels, régulièrement, et sur Windows Update et **autorisez les mises à jour automatiques.**

## L'analyse antivirus, tu activeras !

**Installer un très bon antivirus** (Kaspersky ou BitDefender, les deux meilleurs) et maintenez-le à jour régulièrement. Assurez-vous que le fonctionnement en temps réel et bien activé, c'est le module le plus important de ce type d'applications. Si vous n'avez vraiment pas les moyens, retournez-vous vers les deux ou trois produits **antivirus gratuits mais crédibles** (Windows defender, Kaspersky freemium, Bitdefender freemium).

## A la chasse aux malwares, tu partiras !

**Installer un très bon antimalwares** (Malwarebytes Anti-Malware) contre tout ce qui n'est pas du ressort des antivirus et maintenez-le à jour automatiquement. Assurez-vous que son fonctionnement en temps réel et bien activé. Si vous n'avez vraiment pas les moyens, retournez-vous vers les deux ou trois produits en version gratuite dont la version gratuite de Malwarebytes Anti-Malware. Plus généralement, utilisez, régulièrement (environ une fois par mois), la Procédure de décontamination anti-malwares.

## Que de ton ordinateur, sur ta banque en ligne, tu iras.

**Ne vous connectez jamais à votre banque en ligne depuis un autre ordinateur que le vôtre.**
Lorsque vous avez fini de consulter ou travailler sur votre compte bancaire, n'oubliez jamais de vous ***déconnecter du site de votre banque,*** à l'endroit où se trouvait le bouton de connexion, vous invitant à vous authentifier, il y a maintenant un bouton de déconnexion. Cliquez dessus pour vous déconnecter avant de quitter le site de votre banque, avant de fermer votre onglet ou votre navigateur.

*N'enregistrez jamais vos identifiant et mot de passe dans votre ordinateur, que ce soit dans un fichier ou dans votre navigateur s'il vous le propose.*

Comme pour tous les mots de passe, choisissez-en un «dur» et que vous n'utilisez nulle part ailleurs. N'utilisez aucun mot appartenant à un dictionnaire quelconque (nom commun, nom propre, prénom, patronyme, date, immatriculation, etc. ...).

# Les 11 commandements de l'informatique



## Le navigateur et la navigation, tu protégeras !

**L'architecture même de l'Internet et de la circulation des données comporte, pour des raisons historiques de mise au point de l'Internet, des informations révélatrices sur les internautes et leur navigation.** Des officines en tous genres se sont engouffrées dans l'écoute, l'enregistrement et le stockage illimité de ces informations, et d'autres analysent ces informations pour en déduire les profils de chaque internaute du monde. Cet espionnage «naturel», est renforcé par une modification du comportement des internautes qui se révèlent, volontairement, ou à leur insu, sur les réseaux sociaux et les sites de rencontres.
*Il est ainsi habituel de dire que Facebook sait que vous êtes homosexuel* (parce que vous vous êtes révélé publiquement) *tandis que Google sait que vous avez le sida* (par l'analyse de vos centres d'intérêts, de votre géolocalisation et de vos cercles de connaissances.

## Les trucs gratuits, tu fuiras !

***Lorsqu'un service est gratuit, c'est que vous êtes le produit.***

Quelques personnes et organisations de confiance offrent des produits et services gratuitement, par conviction, par militantisme, etc. ... Ces personnes sont connues et reconnues, par exemple, l'**EFF** (Electronic Frontier Foundation) ou la **CNIL** (Commission Nationale de l'Informatique et des Libertés) ou la **Fondation Mozilla** ou **Mark Russinovich**, ou **XPlode** et son AdwCleaner. Mais, les dizaines de milliers de gadgets gratuits, de prétendus outils d'analyse gratuits, de décontamination gratuite, d'optimisation gratuite, de Keygen, de Crack, etc... *ne sont rien d'autre que des outils, de pillage et espionnage de votre vie privée et de votre navigation sur le Web.*

**Dans les cas plus dramatiques, les bidules gratuits :**

- Servent à transformer votre ordinateur en Zombie intégré dans un BotNet (on estime que 25% de tous les ordinateurs du monde sont des Zombies à l'insu de leurs propriétaires)
- Servent à injecter un Keylogger ou à maintenir une porte dérobée ouverte (Backdoor)
- Servent à lancer des attaques depuis votre ordinateur. En plus, vous n'êtes pas considéré comme une victime mais serez probablement poursuivi en justice pour complicité passive à cause de votre laxisme.
- Servent à faire pénétrer des programmes malveillants plus ou moins sévère dont ceux qui prennent l'ordinateur en otage et demande le paiement d'une rançon sous peine de perte totale et irréversible de toutes les données (ransomware, cryptoware, etc. ...)...

*Avant de télécharger, d'installer, d'utiliser le moindre truc gratuit, faites des recherches et posez des questions sur la fiabilité et la confiance à accorder à ce produit ou service.*

Ne faites jamais confiance sur le Web, c'est un panier de crabes. La confiance est la porte grande ouverte à l'attaque. Posez vos questions sur l'un des forums de confiance. Utilisez les multi-antivirus gratuits en ligne pour l'analyse d'un fichier téléchargé, AVANT de l'ouvrir. Utilisez les antivirus gratuits en ligne pour l'analyse d'un ordinateur AVANT d'ouvrir un truc suspect, que ce soit un fichier exécutable ou un fichier de données.

# Les 11 commandements de l'informatique

3/3

## La totalité des mécanismes publicitaires et de tracking, tu bloqueras !

**Bloquez totalement la publicité et le Tracking avec AdBlock for Firefox, UblockOrigin et Ghostery.**

Selon une étude réalisée par Dasient le 10 mai 2010 et publiée par ZDNet le 18 mai 2010, 1.300.000 publicités malicieuses, piégées, sont vues chaque jour (ce nombre est en augmentation rapide) avec 59% d'entre elles utilisant un « Drive-by download » et les 41% restant conduisant à de faux logiciels de sécurité appelés Fake (Fake Security Software).

Certaines « pseudo publicités « sont très bien rémunérées par les cybercriminels et certain administrateurs vont les privilégier. Elles sont très bien faites, et incitent l'internaute à cliquer dessus. Elles conduisent à des pièges (exemple : Fausses mises à jour Java), servant à l'implantation de portes dérobées (Backdoor) permettant la prise de contrôle à distance de l'ordinateur (BotNet et Zombie), ou vous dirigeant vers des outils d'hameçonnage vous conduisant à révéler ce qui devrait rester caché, comme vos comptes bancaires et identifiants.

## Toutes les cases, tu décocheras !

**Tous les téléchargements, toutes les installations de logiciels et outils, etc. ..., vous tentent avec des «cadeaux» livrés en bundle**, offerts par le développeur du logiciel ou ajoutés par le site de téléchargement, dans une pratique appelée Repacking.

Toutes les cases de ces options, bien évidemment chaudement recommandées, sont précochées. Le seul intérêt de ces Pup (Potentially Unwanted Program), voire de ces adwares, ou hijackers ou crapwares, est de faire gagner de l'argent à celui qui a développé le logiciel que vous installez (il est payé par le développeur du truc installé, au nombre d'installations réussies). Tous ces trucs, au minimum totalement inutiles, mais généralement servant à vous espionner ou à vous bombarder de publicités, doivent être évités à tout prix.

## Tes mots de passe, tu durciras !

**Utilisez des mots de passe de 12 caractères de long minimum, faits de majuscules, de minuscules, de signes spéciaux et de chiffres.** Ces mots de passe ne doivent avoir aucun sens et ne doivent être constitués d'aucun mot existant dans un dictionnaire quelconque. Vous éviterez ainsi de vous faire casser votre mot de passe (force brute, tables arc en ciel, attaque par dictionnaire).

## Ta session, tu fermeras !

**Dès que vous tournez le dos à votre écran, fermez votre session**. Ne jamais laisser votre session ouverte lorsque vous vous absentez, même le temps d'aller à la machine à café et revenir. Ne jamais laisser la connexion Internet ouverte lorsqu'elle ne sert pas – inutile de tenter le diable – inutile de risquer qu'un pirate fasse un scan de vos ports, découvre une faille de sécurité, et l'exploite.