

Les 7 péchés de Windows 7

Avec Windows 7, Microsoft a mis en place un contrôle légal sur votre ordinateur et utilise ce pouvoir pour abuser les utilisateurs d'ordinateurs.

- **Éducation**
- **DRM**
- **Sécurité**
- **Monopole**
- **Standards**
- **Verrouillage**
- **Vie privée**

Péché N° 1 :Éducation

"Donnez un poisson à un homme et vous le nourrissez pendant un jour. Apprenez-lui à pêcher et vous le nourrissez pour la vie."

De plus en plus, les ordinateurs deviendront des outils utiles à l'éducation de nos enfants. Mais aujourd'hui, la plupart des enfants dont l'éducation est liée à l'ordinateur ont appris à n'utiliser que les produits d'une seule entreprise : Microsoft — Microsoft dépense de grosses sommes d'argent dans les lobbys et le marketing afin de fournir l'équipement aux services scolaires.

L'éducation des enfants représente un flux majeur de revenus pour Microsoft, et une opportunité stratégique d'implantation de ses produits dans la vie des futurs adultes. En incitant les écoles à apprendre à leurs élèves l'utilisation de Windows et ses logiciels associés, Microsoft peut aussi susciter chez les parents l'obligation de fournir le même programme à la maison. Dans quel autre domaine voit-on une société capable d'imposer aux enfants, de cette manière, son marketing et ses produits brevetés en tant que matériel obligatoire ?

Beaucoup d'états américains se vantent même de leur collaboration avec Microsoft, tout en ignorant ou se désintéressant de l'influence néfaste a sur leurs gouvernements l'acceptation de cadeaux de la part de cette gigantesque entreprise. Les logiciels de Microsoft étant propriétaires, ils sont **incompatibles** avec l'éducation : les utilisateurs ne sont que de simples consommateurs passifs dans leurs interactions avec Windows, il leur est juridiquement interdit d'adapter le logiciel pour résoudre un problème particulier ou satisfaire une curiosité intellectuelle en examinant son code source. Une éducation utilisant la puissance des ordinateurs devrait être un facteur de liberté et d'autonomie, et non un boulevard pour une entreprise unique inculquant son monopole par endoctrinement.

Le logiciel libre, d'un autre côté, offre aux enfants une voie vers l'autonomie, en les encourageant à explorer et apprendre. Nulle part la promesse d'une plate-forme éducative utilisant les logiciels libres n'a été plus significative que dans le projet One Laptop Per Child (OLPC). Lancé par le professeur du MIT (NDT : MIT = Massachusetts Institute of Technology) Nicholas Negroponte en 2003, OLPC a été conçu dans le but d'apporter aux enfants du monde entier, une formation supérieure en utilisant la combinaison des technologies de l'information et la liberté. Le projet a pour but de produire des appareils peu coûteux (en commençant par le dénommé XO) auxquels des millions d'enfants pourront accéder, et des logiciels libres, afin qu'ils [puissent avoir les libertés essentielles d'exploration et de partage de leurs logiciels](#).

Puis [sous la pression de Microsoft](#), Negroponte est revenu sur l'engagement de liberté du projet en annonçant que les machines fonctionneraient également avec le système d'exploitation non-libre Windows XP.

Microsoft n'est pas la seule menace sur l'éducation : Adobe et Apple se sont tous deux fermement positionnés dans l'éducation, même sous Windows. Les lecteurs propriétaires d'Adobe (Flash, Shockwave) et d'Apple (iTunes, Quicktime) sont très largement utilisés dans le logiciel éducatif.

Microsoft est en train de cibler les gouvernements qui achètent des XO (NDT), en essayant de leur faire remplacer le logiciel libre par Windows. Il reste à voir dans quelle mesure Microsoft va réussir. Mais avec toute cette pression, Microsoft a nui à un projet ayant distribué plus d'un million d'ordinateurs portables fonctionnant sous logiciel libre, et a considéré la plate-forme bon marché comme un instrument pour rendre les enfants pauvres du monde entier dépendants de ses produits. L'OLPC risque de devenir un nouvel exemple du procédé pratiqué par Microsoft pour convaincre les gouvernements mondiaux qu'une éducation s'appuyant sur les ordinateurs doit être synonyme d'une éducation utilisant Windows. Afin d'éviter cela, il est vital que nous travaillions à encourager une prise de conscience générale de la nuisance générée par l'implication de Microsoft dans l'éducation de nos enfants. Une bonne manière de le réaliser est de [télécharger Sugar](#) et d'aider un enfant de votre entourage à expérimenter le logiciel libre.

Comment le logiciel libre s'oppose-t-il à cela ? Liberté 1 : La liberté d'étudier le fonctionnement du programme, et de le modifier pour qu'il exécute votre volonté.

Lecture supplémentaire: [Pourquoi les écoles devraient exclusivement utiliser des logiciels libres](#).

Péché N° 2 : Microsoft aime les DRM.

Les Digital Restrictions Management (DRM) sont des mesures technologiques restreignant ce que les gens peuvent faire avec leurs ordinateurs. [Les DRM sont implantés au coeur de Windows 7, ainsi de nombreux services Microsoft](#) imposent les DRM aux utilisateurs. Dans certains cas, Microsoft a ajouté ces restrictions en suivant les ordres des [sociétés de télévision](#), d'Hollywood et de l'industrie de la musique. Dans d'autres cas, Microsoft [va au-delà des demandes de ces compagnies](#), suggérant que Microsoft utilise les DRM uniquement pour créer un verrouillage. Que Microsoft soit simplement de mêche avec les grandes sociétés de médias ou qu'elle défende les DRM pour ses propres intérêts, le résultat pour les utilisateurs de logiciels est le même...

La peur [monomaniaque](#) des [grandes entreprises de médias](#) est que les gens partagent l'information numérique avec leurs amis, bâtissant une bibliothèque publique et libre de biens culturels. Les bibliothèques publiques sont des institutions merveilleuses et, dans une ère numérique, elles en deviennent presque miraculeuses : nous pouvons maintenant offrir un accès universel à la connaissance et la culture humaine - ou au moins à tout ce qui a été publié - à coût réduit, voire nul. Ce qui est incroyable, c'est que c'est presque automatique : dès que l'on peut partager librement avec des amis via un réseau mondial, on a une bibliothèque publique numérique. Les réseaux P2P en sont un exemple et le Web un autre. La valeur de ces bibliothèques pour le public est historique et incommensurable. Mais les sociétés de médias servent des actionnaires, pas le public, en conséquence, elles sont prêtes à détruire toute ressource publique naissante qui pourrait empiéter sur leurs profits. L'ordinateur personnel a été conçu dès ses origines pour rendre le partage d'information facile et rapide, donc pour que les sociétés de médias puissent restreindre le partage, elles ont besoin de l'entière collaboration et à tous les niveaux des fabricants de logiciels. Nous voilà chez Microsoft.

Afin d'empêcher complètement le partage, les sociétés de médias avaient besoin que Microsoft fasse deux choses :

- Premièrement, elles devaient s'assurer que tout signal numérique sortant soit verrouillé comme pour les fichiers "DRMisés" de films ou de musique. Sinon, vous pourriez tout simplement visionner une vidéo sur votre ordinateur connecté à un autre appareil (comme votre caméra numérique) et appuyer sur enregistrer. C'est pourquoi, quand Windows lit un fichier avec DRM, il doit constamment vérifier que tout appareil connecté coopère avec la combine des DRM. Cette anti-fonction est appelée [Protected Media Path](#) (chemin du média protégé). Microsoft l'a introduit dans Vista et continue avec Windows 7.
- Deuxièmement, les sociétés de médias avaient besoin que Microsoft empêche les autres programmes de surveiller le processus de lecture et d'intercepter le son et l'image sous une forme non chiffrée. Après tout, c'est encore votre ordinateur, et (d'autant plus que les sociétés de médias haïssent cela) vous pouvez installer et exécuter n'importe quelle application voulue. Vista et Windows 7 comblent cette "lacune" en surveillant toutes les applications en fonction dès qu'un fichier protégé avec DRM est lu. Si Vista ou Windows 7 détectent une application non-homologuée tournant en arrière plan, votre chanson ou votre vidéo s'arrêtera, tout simplement. Dans la pratique, le chiffrement de la plupart des types de DRM ont été contournés (y compris DVD et Blu Ray), et des copies sans DRM de pratiquement toutes les musiques ou vidéos sont disponibles sur l'Internet. Mais les utilisateurs de Windows 7 et Vista ont toujours du code qui tourne sur leurs ordinateurs - en tout temps - essayant de limiter leurs droits fondamentaux à partager l'information avec d'autres et leur facultés à construire des bibliothèques.

Ces restrictions ont dépassé tout ce que l'on pouvait attendre. Par exemple, à la demande de NBC, Microsoft a empêché les utilisateurs de Windows Media Center d'enregistrer des spectacles télévisés, ceux que NBC souhaiterait que vous n'ayez pas, même si ce type d'enregistrement est une fonctionnalité incluse dans Windows Media Center. Elle prétend simplement suivre les régulations de la FCC (NDT: Commission fédérale des communications) alors que la Second Circuit Court of Appeals (NDT : Cour d'appel aux États-Unis d'Amérique) juge que la FCC n'a aucune autorité pour produire de tels règlements.

Microsoft ajoute même des DRM dans des contextes que les sociétés de médias ont pourtant massivement abandonnés. Cette année, alors que toutes les principales boutiques de musique ont adopté le "sans DRM", Microsoft a lancé une boutique de musique en ligne pour téléphone mobile bourrée de DRM. Ce service de musique possède en particulier une séduisante limitation : de nombreuses personnes changent de mobile aux six mois ou chaque année, or il n'y a aucun moyen de transférer les chansons d'un téléphone à l'autre. Si vous changez de téléphone tous les six mois, alors vous perdez votre musique tous les six mois. Mais plus important, c'est un niveau de DRM, que les sociétés de musique n'exigent plus, indiquant que Microsoft a un objectif personnel en défendant les DRM : le verrouillage. Parce que les DRM créent une incompatibilité artificielle, c'est l'outil parfait pour lier l'utilisateur d'un service à un produit particulier. Quand les gens achètent de la musique via un service Microsoft, ils ne peuvent plus utiliser d'autres lecteurs de musique (comme l'iPod par exemple). Même lorsque Microsoft lança son propre lecteur de musique "Zune", celui-ci ne lisait pas les titres protégés avec le DRM "Plays For Sure" de Microsoft vendus par d'autres services de musique (y compris le MTV URGE Music Service implanté dans Windows Media Player 11). La pression des grandes sociétés de médias n'est pas l'unique raison qui pousse Microsoft à défendre les DRM : le verrouillage est fondamental dans sa stratégie commerciale et les DRM sont une bonne manière d'y parvenir.

Microsoft n'est pas la seule société coupable de cela. Apple via [les logiciels iTunes](#), et ses équipements tels les Macintosh, iPod, [iPhone](#) ou Apple TV, impose aussi des DRM aux utilisateurs. Adobe et Sony imposent aussi des DRM aux usagers. Mais Microsoft est un acteur particulièrement agressif pour les DRM et l'intégration des DRM aux plus profonds niveaux de Windows 7 est une raison majeure de ne pas l'acheter.

Le logiciel libre, de par sa nature propre, ne soutient pas les DRM. Si des DRM étaient ajoutés au logiciel libre, les utilisateurs et les développeurs bricoleraient autour et les supprimeraient.

Lecture supplémentaire : [S'opposer aux Digital Right Management](#)

Péché N° 3 : La sécurité

«La sécurité d'un ordinateur et d'un réseau dépend de 2 choses : Ce que vous faites pour sécuriser votre ordinateur et votre réseau, et ce que tous les autres font pour sécuriser leurs ordinateurs et leurs réseaux. Ce n'est pas suffisant que vous mainteniez un réseau sécurisé. Si les autres n'entretiennent pas leur sécurité, nous sommes tous plus vulnérables aux attaques. Lorsque de nombreux ordinateurs non-sécurisés sont connectés à Internet, les vers se répandent plus rapidement et plus largement, les attaques distribuées de type déni-de-service sont plus faciles à déclencher, et les spammeurs ont plus de plate-formes à partir desquelles envoyer des courriels. Si la sécurité de l'ordinateur moyen sur internet se dégrade, la sécurité de votre ordinateur suivra.

-- Bruce Schneier

Mais comment savoir que votre ordinateur est sûr ? Si vous utilisez du logiciel propriétaire, vous ne le pouvez pas ! Avec le logiciel libre, même si vous ne disposez pas des compétences nécessaires à l'analyse du logiciel, vous pouvez être certain que quelqu'un d'autre en dispose.

Windows a une longue histoire de vulnérabilités, permettant la diffusion de virus et la prise de contrôle d'ordinateurs pour en faire des robots expéditeurs de spams. Parce que le logiciel est secret, tous les utilisateurs sont dépendants de Microsoft pour corriger ces problèmes, mais Microsoft a en tête ses propres intérêts liés à la sécurité, pas ceux de ses utilisateurs.

En 2005, [une vulnérabilité](#) a été découverte, qui affectait toutes les versions de Windows à partir de Windows 3.0, publiée en 1990, jusqu'à Windows Server 2003 R2 publiée en décembre 2005, Windows XP et les versions les plus récentes étant particulièrement touchées. Le problème touchait le format d'image Windows Metafile, un format couramment utilisé pour les cliparts ou autres images vectorielles. Les fichiers contenant des codes d'échappement spéciaux permettent l'exécution de code arbitraire défini par un utilisateur, lorsque l'affichage de l'image échoue.

Le chercheur en sécurité [Steve Gibson](#) pense que ce défaut pourrait également être intentionnel.

Les situations dans lesquelles ces fichiers sont vus sont très nombreuses

- Consulter un site Web avec Internet Explorer
- Prévisualiser une image sur votre ordinateur ou en utilisant l'explorateur de Windows.
- Prévisualiser un courriel infecté dans Microsoft Outlook ou Outlook Express.

Microsoft a même introduit une nouvelle variété de logiciel malveillant, le macro virus, permettant apparemment à d'innocents tableaux ou documents texte de contenir du code malicieux dans Microsoft Office.

Une partie du problème de sécurité de Windows provient du fait que par défaut, les comptes administrateurs sont utilisés et attendus par de nombreuses applications. Ces comptes administrateurs permettent également aux logiciels malveillants d'attaquer le système d'exploitation.

Dans le logiciel libre, cela serait traité à la fois comme un incident technique et comme un problème social. Si le logiciel a besoin de mener des actions en tant qu'administrateur, il faut une bonne raison de le faire, et, si cela empêche les utilisateurs de faire leur travail sans risque pour leur vie privée ou leur sécurité, c'est anti-social.

VIXANE vous donne le pouvoir
sur vos ordinateurs

Téléphone: 06 09 41 76 89

Mail: francois.deguerry@vixane.fr

Internet: vixane.fr

Péché N° 4 : Le monopole de Microsoft

Microsoft a été jugé coupable de comportement monopolistique partout dans le monde. Avec Windows Vista, Microsoft a travaillé avec les fabricants de PC pour augmenter de manière significative les spécifications matérielles nécessaires à une expérience utilisateur standard, poussant les gens à faire l'acquisition de nouveaux ordinateurs pour faire fonctionner le système mis à jour. Le monopole de Microsoft affecte votre liberté.

Les premières version de Windows 3.1, s'appuyant sur une version du système d'exploitation DOS, [renvoyaient une erreur](#) si un DOS non Microsoft, tel que DR-DOS de Digital Research, était détecté. Le PDG de Microsoft, Bill Gates, a un jour déclaré dans un message interne : "Vous ne m'avez toujours pas donné de réponse à la question de savoir ce qui ferait qu'une application fonctionnerait sous MS-DOS et pas sous DR-DOS. Existe-t-il une fonctionnalité qu'ils auraient pouvant nous servir à ça ?". De même, le vice président de Microsoft Brad Silverberg a envoyé un autre message, indiquant : "L'utilisateur est supposé se sentir mal à l'aise, et lorsqu'il rencontre des dysfonctionnements, suspecter que le problème est DR-DOS, et sortir acheter MS-DOS."

Microsoft a récemment essayé de vendre un ensemble de brevets qui mettraient GNU/Linux en danger de violation de brevet : ces brevets ont [finalement été achetés par le réseau Open Innovation](#), un groupe acquéreur de brevets pour protéger le logiciel libre.

Ces derniers mois, nous avons vu qu'Amazon.co.uk commence à [rembourser Windows rapidement et facilement](#) aux utilisateurs de GNU/Linux faisant l'acquisition d'un netbook. Cela deviendra-t-il une tendance croissante, qui sait ?

Pire, la plupart des fabricants de PC ne vous offrent toujours pas la possibilité d'acheter une machine sans Windows.

Traditionnellement, composer votre propre machine était une façon de contourner la taxe Windows. Microsoft a réussi à inverser cette tendance également. Sur des sites tels que NewEgg, de nombreuses offres promotionnelles sont liées à l'achat d'une version OEM de Windows, pénalisant ainsi ceux qui cherchent activement à éviter Microsoft et d'autres entreprises de logiciels propriétaires, au nom de la liberté.

Le monopole de Windows n'est pas seulement limité à l'influence directe des produits de Microsoft : de nombreux fabricants d'ordinateur ne livrent leurs machines qu'avec Windows, à cause d'offres liées à d'autres entreprises de logiciels, chargeant la machine d'un ensemble de logiciels propriétaires, et intégrant des offres d'essai de fournisseurs d'accès Internet ou d'autres camelote.

Le logiciel libre n'a pas ce problème : Il ne peut exister de monopole dans le logiciel libre, parce que chacun dispose du code source, et tout le monde peut modifier le logiciel et distribuer les versions modifiées. Bien que certains fabricants majeurs de PC envisagent de vendre des machines équipées de GNU/Linux, tous les fabricants majeurs de PC sont toujours de fervents promoteurs de l'usage des logiciels propriétaire, en vertu de leur relation avec Microsoft.

En savoir plus: [Le procès anti-trust de Microsoft et le logiciel libre](#)

Péché N° 5 : Microsoft s'oppose aux standards...

Les standards sont importants. Avec les standards, les utilisateurs de plate-formes variées peuvent partager des informations. Ils permettent également aux utilisateurs de s'affranchir des verrous mis en place par les éditeurs. C'est particulièrement vrai dans le domaine des documents bureautiques, où des gouvernements entiers, aussi bien nationaux que régionaux, ont pris des décisions sur la pérennité de leurs informations dans le futur.

Microsoft tente de bloquer un format ouvert, établi et libre en poussant lourdement celui sur lequel ils ont plus de contrôle, et ils utilisent tout leur pouvoir de lobbyiste pour essayer de l'engager en urgence dans le processus de standardisation, en détruisant la réputation des organes de standardisation auprès de qui ils cherchent l'approbation. Microsoft défie le standard existant des documents bureautique avec son propre format Office OpenXML, qui intègre spécifiquement Microsoft Office, plutôt qu'un standard plus générique.

Au contraire d'OpenDocument qui est, bien supporté et multiplateforme le format de Microsoft n'est pris en charge que par le logiciel propriétaire d'un seul éditeur, et parce qu'il a été conçu pour absorber chaque dysfonctionnement, problème technique et fonctionnalité historique du logiciel Office de Microsoft, les spécifications d'OOXML font plus de 6000 pages, rendant beaucoup plus complexe l'implémentation dans d'autres logiciels.

Les documents de bureautique ne sont pas le seul domaine dans lequel Microsoft s'insurge contre les standards. Microsoft a abusé de son monopole sur Internet, en ne rendant son navigateur Internet Explorer compatible qu'avec une partie des standards du Web, soumettant ainsi les utilisateurs à une expérience dégradée comparée à celle obtenue avec un navigateur alternatif. En Europe, Microsoft a été contraint d'offrir aux utilisateurs un écran de choix de navigateurs alternatifs lors de l'installation de Windows 7, on a voulu mettre fin à son monopole sur les navigateurs.

Avec les formats libres, il est important de s'assurer que vous utilisez du logiciel libre également. Les formats libres ne peuvent excuser les dommages causés par le logiciel propriétaire.

Péché N° 6 : La stratégie de verrouillage de Microsoft

« **Étreindre, étendre et exterminer** », telle est la description par Microsoft de la stratégie de verrouillage de ses utilisateurs par les extensions propriétaires en tant que norme.

Microsoft [tente régulièrement de forcer les mises à jour](#) de ses clients, en supprimant le support des versions anciennes de Windows et Office, tout en changeant les formats de fichiers utilisés par ses applications de bureautique, laissant de nombreux professionnels dans une situation où ils n'ont d'autre choix que de mettre à niveau pour continuer à utiliser les logiciels et les formats de documents dans lesquels ils ont investis du temps.

En [retirant le support](#) du système d'exploitation ou d'autres logiciels, tels que Microsoft Office, Microsoft laisse les entreprises sans autre possibilité que de mettre à niveau vers les versions les plus récentes de ses logiciels. Les versions récentes du logiciel ont des formats de fichiers qui diffèrent des versions précédentes, contraignant les entreprises qui échangent ces documents à procéder également à une mise à jour. Qui plus est, certaines applications refusent de fonctionner sur d'anciennes versions de Microsoft Windows, obligeant à réaliser des mises à jour complètes de systèmes pour ce qui est essentiellement un format d'échange de document.

Ce comportement n'est pas limité à Microsoft, mais également aux entreprises de logiciels propriétaires qui produisent pour Windows. Adobe [met à jour régulièrement ses logiciels](#), afin d'annihiler les méthodes utilisées pour contourner les mesures restrictives de ses lecteurs de PDF, de même, Apple a utilisé [son application de mise à jour](#) sur Windows [pour contraindre les utilisateurs d'iTunes à installer le navigateur Web Safari](#).

Voici comment le logiciel libre a résolu ce problème : tous ceux qui utilisent ce logiciel ont accès au code source, créant trois possibilités d'apporter du support au logiciel, au delà de tout support qui peut être proposé par les développeurs du logiciel. Premièrement, un ensemble d'utilisateurs du logiciel décide de continuer à supporter lui-même le produit avec des mises à jour et des corrections de bugs. Un groupe appelé Fedora Legacy a agi ainsi pour Red Hat 7.3 et Red Hat 9, durant plusieurs années après que les mises à jour officielles ont cessé. Deuxièmement, un nouveau projet peut décider de continuer à développer lui-même le logiciel, offrant ainsi aux utilisateurs une option alternative de mise à jour sous la forme d'une nouvelle version ou distribution du logiciel. Enfin, l'utilisateur peut engager un développeur indépendant, ou une équipe de développeurs pour continuer à améliorer et à maintenir le logiciel.

Péché N° 7 :Microsoft et la vie privée

À qui votre ordinateur devrait-il obéir ?

La plupart des gens pensent que leur ordinateur devrait leur obéir, plutôt qu'à quelqu'un d'autre. Pourtant, grâce à un projet appelé «[Informatique de confiance](#)» (NDT : En anglais Trusted computing and software) qu'ils ont appelé [Windows Genuine Advantage](#), Microsoft et d'autres ont projeté que votre ordinateur leur obéisse plutôt qu'à vous, et cela a de sérieuses conséquences sur votre vie privée.

Windows Genuine Advantage (WGA) est le système permettant à Microsoft de vérifier votre ordinateur à distance. WGA parcourt diverses parties de votre disque dur afin d'assurer à Microsoft que vous utilisez une version «approuvée» de Windows. WGA surveille obligatoirement le système, et si Microsoft décide que vous n'êtes pas «approuvé», il lui est possible de désactiver des fonctionnalités de votre ordinateur. Actuellement, [Microsoft confirme que WGA vérifie](#) :

- Le fabricant et le modèle de l'ordinateur
- le BIOS
- l'adresse MAC
- Un numéro unique associé à l'ordinateur - GUID pour Globally Unique Identifier (NDT : Identifiant globalement unique)
- Le numéro de série du disque dur
- Les paramètres régionaux et de langue du système d'exploitation
- La version du système d'exploitation
- Les informations du BIOS, telles que le fabricant, la version, la date
- Le fabricant du PC
- Les paramètres locaux de l'utilisateur
- Les résultats de l'installation et de la validation
- Les clés d'identification de Windows ou de Microsoft Office
- L'identifiant produit de Windows XP

WGA est responsable d'un grand nombre de problèmes liés à la vie privée, y compris la suppression de logiciels. WGA est mis à jour automatiquement lors des mises à jour critiques de Microsoft, n'offrant aux utilisateurs que peu de choix, si ce n'est d'accepter les changements apportés au système que Microsoft est capable de contrôler. Nombreux sont ceux qui ont déclaré que WGA est un spyware (NDT : logiciel espion), eh bien que Microsoft s'en défende, elle conserve le pouvoir de décider ce qui relève d'une intrusion dans votre vie privée.

Pour Windows 7, ils ont changé le nom de ce produit en Windows 7 Activation Technologies (WAT), mais la fonctionnalité reste la même.

La vision de Microsoft d'une "informatique de confiance" est appelée [Palladium](#). Les programmes propriétaires ont auparavant intégré des fonctionnalités malveillantes, mais Palladium vise à les rendre universelles.

Hollywood et les entreprises musicales [adopteront Palladium pour s'assurer](#) que les vidéos et les musiques que vous téléchargez ne peuvent être jouées que sur un ordinateur particulier, et le partage de fichiers « autorisés » sera totalement impossible.

Rendre le partage impossible est déjà suffisamment mauvais, mais ce n'est pas le pire. Des [projets existent, afin d'utiliser la même fonction pour le courriel et les documents](#), menant à des courriels qui disparaissent en deux semaines, ou à des documents qui [ne peuvent être lus que sur les ordinateurs](#) d'une seule entreprise.

Imaginez que vous receviez un courriel de votre patron vous demandant de faire quelque chose que vous pensez risqué : un mois plus tard, lorsque la situation se retourne, vous ne pouvez pas utiliser le courriel pour démontrer que cette décision n'était pas la vôtre. "Obtenir un écrit" ne vous protège pas lorsque l'ordre est écrit à l'encre sympathique.

[L'informatique perfide](#) met en danger l'existence des systèmes d'exploitation et des applications libres, parce que vous pourriez même ne pas pouvoir les faire fonctionner.

Certaines versions de l'informatique perfide nécessiteront que le système d'exploitation soit spécifiquement autorisé par une entreprise particulière. Les systèmes d'exploitation libres ne pourront pas être installés. Certaines versions de l'informatique perfide nécessiteront que chaque programme soit autorisé par le développeur du système d'exploitation.

Vous ne pourriez pas faire fonctionner des applications libres sur de tels systèmes. Si vous découvriez comment le faire, et en parliez à quelqu'un, cela pourrait constituer un crime.

© 2009 Free Software Foundation, Inc

VIXANE vous donne le pouvoir
sur vos ordinateurs

Téléphone: 06 09 41 76 89

Mail: francois.deguerry@vixane.fr

Internet: vixane.fr