MAINTENANCE INFORMATIQUE

Les DANGERS Les PANNES Les SOLUTIONS

Les DANGERS

Sécurité informatique des fourmis contre les vers !

Publié le 11 octobre 2009

La nature fait bien les choses ! Nos experts en sécurité informatique commencent à le comprendre et s'en inspirent ! ainsi des fourmis digitales vont lutter contre des vers informatiques ! On aura tout vu …
La fourmi est une petite bête résistante. elles s'adaptent facilement aux menaces pendant qu'elles travaillent. alors, pourquoi ne pas sen inspirer ?
C'est ce qu'ont réalisés des chercheurs américains de l'Université Wake Forest. Et voilà des petites fourmis informatiques qui se baladent dans les réseaux pour détecter une éventuelle menace ! Dès qu'il y en a une de repérée, la fourmi appelle en renfort ses collègues, ce qui attire l'attention de l'informaticien … tout simplement ! C'est ce qu'on appelle l'intelligence collective ! Il suffisait d'y penser.

Les crimes informatiques augmentent de 276% en 2009

nouvelobs.com | 02.10.2009 | 14:27

Failles, fuites et autres vulnérabilités sont de plus en plus exploitées par les pirates.
Le vol de renseignements confidentiels augmente de 75% sur l'année, six fois sur 10 via un virus.

Une étude canadienne met en lumière l'explosion du nombre de failles, fuites et autres vulnérabilités en 2009, a-t-on appris vendredi 2 octobre. **Le crime informatique aurait augmenté de 276%** par rapport à 2008, entraînant le doublement des coûts en sécurité informatique, avec une facture s'élevant à 834.000 dollars pour le seul Canada.
Si les cibles préférées des pirates informatiques restent les organes gouvernementaux, les sociétés cotées en Bourse accusent une hausse de 6% des attaques informatiques.
Au total, l'accès non autorisé aux informations des employés augmente de **112%**, de même que le vol de renseignements confidentiels croît de **75%**, six fois sur dix grâce à **un virus**.

Après Hotmail, GMail et Yahoo! visés par des pirates

Des attaques de **"phishing"** ont été recensées par les deux messageries électroniques, qui demandent à leurs utilisateurs d'être prudents.

Mis à jour le 07/10/2009 - 10h03

Personne n'est épargné. Lundi, **Microsoft Hotmail** était victime de pirates. Mardi, ce sont ses deux principaux rivaux, **Google Mail** et **Yahoo!** Mail qui ont été la cible des hackers. "*Nous avons récemment été avertis d'attaques de phishing via lesquelles des pirates informatiques se sont procurés des données pour accéder à des adresses électroniques*", a indiqué Google, précisant qu'un "*petit nombre*" de comptes Gmail étaient concernés. "*Aussitôt que nous avons eu connaissance de l'attaque, nous avons lancé une remise à zéro des comptes affectés*", a ajouté Google.

La technique de "*phishing*", ou hameçonnage, consiste à tromper les utilisateurs pour leur extorquer des informations ou les inciter à télécharger des logiciels malveillants. Parmi les tactiques utilisées figure l'envoi de courriers électroniques frauduleux, assortis par exemple de pièces jointes promettant des photos de célébrités dénudées. Une attaque a également touché un "*nombre limité*" de comptes **Yahoo!**, a indiqué l'entreprise dans un communiqué, soulignant que le *"phishing et autres arnaques en ligne*" étaient un "*problème*" concernant tout le secteur.

AOL, filiale internet de Time Warner et autre important fournisseur d'adresses électroniques, a de son côté indiqué "*surveiller de près la situation*". Lundi, **Microsoft** avait annoncé avoir bloqué l'accès à des milliers de comptes de ses messageries électroniques **Hotmail**, dont les mots de passe avaient été identifiés par des pirates informatiques qui les ont livrés en pâture sur internet. **Microsoft**, Google et **Yahoo!** ont assuré que leurs bases de données n'avaient pas été affectées et appelé les utilisateurs à suivre les règles élémentaires en matière de sécurité informatique: ne pas cliquer sur des liens suspects, installer et mettre à jour un logiciel antivirus, se méfier des pièces jointes non sollicitées.

Un cheval de Troie qui pille votre compte bancaire

Une société de sécurité informatique a identifié un programme malicieux qui puise dans les comptes en banque en camouflant l'opération.

01net 30/09/2009 à 16h15

Généralement, les malwares de type cheval de Troie s'installent sur les ordinateurs pour transmettre à des escrocs des données personnelles telles que logins, mots de passe, e-mails, numéros de compte. Elles seront utilisées dans un deuxième temps pour accéder à des comptes privés en ligne. Mais il y a maintenant plus direct : un virus qui, une fois installé, pompe votre argent directement depuis votre compte bancaire.

C'est la société californienne Finjan, spécialiste en sécurité informatique, qui l'a identifié. Elle le décrit dans un rapport sur le cybercrime qui vient d'être publié. Ce cheval de Troie vise pour l'instant les clients de banques allemandes. Son principe est simple et assez terrifiant.

Tout commence comme souvent avec les virus : un e-mail avec un lien vers un site Internet. Le site peut être soit un vrai site, mais déjà infecté, soit un site conçu exprès pour piéger l'internaute.

En cliquant et en arrivant sur les sites concernés, ce dernier active sans le savoir un code malicieux. Celui-ci exploite une faille de sécurité du navigateur et installe sur l'ordinateur un programme, appelé URLzone bank, conçu pour communiquer avec les sites de banques pendant la session de connexion.

438 000 euros volés en 22 jours

A partir de là, l'escroc envoie à partir d'un serveur ses instructions au programme malicieux qui lui retourne des informations. Il peut alors connaître l'état du compte (crédits, débits), les opérations effectuées (transferts, virements, etc.) et, plus important, extraire des sommes.

Mais cela va plus loin. Avec toutes ces informations, les escrocs peuvent s'assurer qu'ils pillent un compte qui n'est pas déjà à découvert. Ensuite, ils prennent soin de ne pas retirer de sommes trop importantes. C'est le programme qui calcule lui-même la somme adéquate. Tout ceci afin de ne pas alerter les systèmes de sécurité de la banque en procédant à des retraits anormaux ou à la régularité inhabituelle. Après quoi, le programme ordonne un virement vers un compte contrôlé par les escrocs.

La méfiance de l'utilisateur est elle aussi endormie grâce à de faux relevés bancaires produits par le cheval de Troie ! En consultant ses relevés de compte en ligne depuis l'ordinateur infecté, la victime de ce piratage ne s'apercevra de rien. En revanche, si cette consultation s'opère depuis une autre machine, le problème sera visible. Tout n'est pas perdu...

Les sommes détournées atterrissent sur des comptes de « mules », et non sur les comptes des escrocs eux-mêmes. Les « mules », comme dans les arnaques du monde physique, sont des passeurs occasionnels, embauchés pour participer à une arnaque, et payés avec une commission sur le produit global du forfait.

D'après Finjan, 438 000 euros ont été ainsi volés en 22 jours courant août, à partir de quelques centaines d'ordinateurs, même si plus de 6 000 machines ont été infectées.

Pour éviter tout problème, le premier réflexe doit être toujours le même : ne pas ouvrir d'e-mails douteux, en provenance d'expéditeurs inconnus, ne pas cliquer sur des liens dont vous ne connaissez pas l'origine. Et, dans le cas qui nous occupe, consulter de temps en temps votre compte en ligne depuis un ordinateur diffférent du votre...

Le mot de passe Hotmail le plus courant est...

Publié le 11/10/2009

La semaine dernière, 20.000 comptes Hotmail étaient piratés. L'occasion de redonner des règles de bon sens quand à la création d'un mot de passe car...

La révélation du piratage de 20.000 comptes Hotmail a permis une petite analyse de ces comptes piratés. Et il apparaît que les utilisateurs de comptes Hotmail (mais cela doit aussi s'appliquer aux autres comptes de messagerie) ne sont pas très prudents. En effet, le mot de passe le plus utiliser est... "123456". Pour l'originalité, on repassera. Pire encore : le second mot de passe le plus utilisé est "123456789". Autant dire qu'il est alors facile pour un pirate de pénétrer votre compte.

Le bon sens veut que l'on change régulièrement de mot de passe, rappellent les société spécialisées dans la sécurité informatique. Et elle conseillent d'utiliser des mots de passe longs, contenant des lettres et des chiffres et si possible des minuscules et des majuscules. Mieux encore, si l'éditeur du site les autorisent : utilisez des caractères spéciaux comme "(" ou "-"... votre mot de passe sera d'autant plus sûr

Mise à jour du 6 octobre 2009

Suite à l'apparition de courriers électroniques véhiculant un faux message de l'administration des impôts, le ministère du Budget monte au créneau. Il publie un communiqué ce 6 octobre pour alerter les internautes qu'il s'agit d'une **arnaque de type « phishing »**. « *La direction générale des finances publiques, totalement étrangère à cet envoi, rappelle qu'en aucun cas elle ne fait des envois de ce type aux contribuables pour leur demander des informations. Par ailleurs, le numéro de carte bancaire n'est jamais exigé pour le paiement d'un impôt ou le remboursement d'un crédit d'impôt. »* indique le communiqué. Il est donc fortement déconseillé de répondre à ce courriel.
Mais la Direction des Impôts va plus loin. Elle demande aux internautes de lui transmettre les e-mails frauduleux en question pour étayer *« l'action judiciaire qu'[elle] entend engager. »*

Première publication le 5 octobre 2009

Le « phishing » qui promet une réduction d'impôts

Un e-mail censé provenir du ministère du Budget promet aux internautes un remboursement d'impôt. Il s'agit d'une arnaque de type hameçonnage.

Vous en rêvez, le ministère du Budget le fait : vous allez être remboursé de 178,80 euros sur vos impôts. C'est un courriel qui vous le dit. Mais pour obtenir cette somme, il faut cliquer sur un lien dans le message et remplir le formulaire qui s'affiche. Si vous ne l'avez pas déjà compris, sachez qu'il ne faut rien faire de tout cela !

Ce message est en effet une arnaque de type *phishing* (ou hameçonnage) actuellement en circulation. Plutôt bien réalisé, il arbore le logo « officiel » République française, semble provenir de la Direction générale des finances publiques, est signé Philippe Berger, conciliateur fiscal adjoint (avec signature manuscrite), et porte en bas de page un « copyright » ministère du Budget, des Comptes publics et de la Fonction publique.

Le texte annonce que *« vous êtes admissible à recevoir un remboursement d'impôt »*. Pour en bénéficier, vous devez seulement remplir un formulaire et attendre dix jours ouvrables que votre dossier soit traité.

Une arnaque globalement bien conçue

Une page imitant celles du site des impôts

Ledit formulaire est accessible par un lien qu'il vous suffit d'activer directement depuis l'e-mail. **C'est là que réside le danger : ce lien vous amène à une page imitant celle du site impots.gouv.fr**. Vous devez y saisir votre nom, votre numéro de carte bancaire et votre code PIN.

Premier problème, l'adresse du site n'est pas sécurisée, en https, et est pour le moins fantaisiste (elle commence par une série de chiffres). Ensuite, on vous demande votre numéro de carte bancaire et le code que vous devez composer au guichet pour retirer de l'argent ! Autant aller vous jeter dans la gueule du loup...

L'internaute prudent aura aussi noté des maladresses de formulation dans le libellé de l'e-mail, qui trahissent une origine douteuse du message (*« s'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre... »*). Mais dans l'ensemble, l'arnaque est plutôt bien conçue, soignée et, pour une fois, sans faute de français. Il est vrai que depuis quelques temps, les e-mails de *phishing* sont de plus en plus confondants de réalisme. D'où le danger.

Toujours les mêmes précautions à prendre

Une première vague d'hameçonnage aux couleurs du ministère du Budget a circulé à la fin du mois de septembre 2009, comme le révélait à l'époque le site spécialisé dans la sécurité informatique Zataz.com. La nouveauté, ici, réside dans la fabrication d'une fausse page du site des impôts.
Les précautions à prendre sont toujours les mêmes : **ne pas cliquer sur un lien dans un courriel douteux, ne pas saisir de données personnelles et bancaires sur une page non sécurisée**, toujours passer par la page d'accueil d'un site si vous voulez saisir de telles données et ne pas faire d'opérations administratives, bancaires ou autres directement depuis un e-mail. Le site d'information juridique Juritel décrit ici la marche à suivre pour détecter une arnaque de ce genre.
Ces dernières relèvent en tout cas du code pénal et peuvent être punies de cinq ans d'emprisonnement et de 375 000 euros d'amende.
Et si jamais vous vous tombez dans le panneau, sachez que **vous pouvez avoir des problèmes pour vous faire rembourser par votre banque**. En effet, dans ce genre d'arnaque, c'est vous qui, de votre plein gré, fournissez vos données bancaires. De plus, les banques ont pris l'habitude de communiquer et d'alerter leurs clients sur les dangers du *phishing*. Alors prudence

Quand les Russes jouent aux pirates

Gilles Gaetner le jeudi, 01/10/2009

La justice enquête sur des hackers qui se sont introduits dans des banques françaises. Notamment au CIC-Crédit mutuel.

Plus de 600 banques dans le monde fragilisées par des tentatives de piratage. Une vingtaine en France qui n'ont pu y échapper. Quelques centaines de milliers d'euros pillés à des clients (130 en tout) aussi incrédules que consternés. Auteurs de l'arnaque recherchés par Interpol : des pirates informatiques russes ou ukrainiens, des hackers, originaires de Kiev, d'Odessa et même d'Omsk (Sibérie). Leurs complices : quelques Français appâtés par des gains faciles. Une trentaine d'entre eux sont actuellement mis en examen

29.09.09 - 11:10

Il est bien loin, le temps où l'internet était réservé à quelques jeunes férus d'informatique. Aujhourd'hui, tout le monde s'y met, s'y est mis ou s'apprête à s'y mettre. Tout le monde, y compris les jeunes retraités.
Sauf que l'internet n'est pas forcément un chemin de roses. Qu'il y a des écueils à éviter, des pièges à flairer et des arnaques dans lesquelles il ne faut pas tomber.
Jacqueline a un ordinateur. Elle est curieuse, mais reste prudente. "*Quand on ne connaît pas, on ne clique pas*". C'est pourquoi Jacqueline n'ouvre jamais de mails en provenance d'inconnus, n'achète rien sur les sites de vente aux enchères, ne divulgue jamais ses données et, si elle va voir les sites de voyage, ne donne jamais son numéro de carte de crédit pour réserver : elle paie à l'arrivée à l'hôtel.

Prudence

Olivier Bogaert, de la Computer Crime Unit, ne leur donne pas tort : "*On n'est jamais trop prudent sur l'internet*", explique-t-il. Et il rappelle le b.a.ba de la sécurité, bon à savoir à tout âge :

- Gardez votre système à jour en effectuant régulièrement les mises à jour suggérées par le concepteur des logiciels utilisés.
  Effectuez aussi régulièrement les mises à jour de votre anti-virus.
  Si vous recevez un mail qui semble provenir de votre banque et vous demande de réintroduire vos données personnelles, jetez-le, c'est une tentative d'arnaque.
- En règle générale, toutes les règles de prudence que vous respectez dans le monde réel, vous devez encore plus y être attentif dans l'univers virtuel.
  Vous hésitez sur la fiabilité de tel ou tel site ? N'hésitez pas à consulter les forums. En tapant dans un moteur de recherche le nom du site et le mot forum, vous trouverez rapidement des sites où les internautes donnent leur avis et, bien entendu, tirent la sonnette d'alarme en cas de fraude.
- Vous recevez un mail au sujet d'un enfant très malade, ou disparu, ou qui a besoin d'une transplantation ? Avant de cliquer sur "renvoyer à tout mon carnet d'adresse", un petit tour sur www.hoaxbuster.com (qui, malgré son nom, est un site francophone) vous permettra de savoir si cet appel est vrai ou plutôt bidon. Généralement, ils entrent dans cette dernière catégorie.
- Si vous tombez, sur un site d'enchères ou dans votre courrier, sur une offre qui a l'air trop belle pour être vraie, dites-vous qu'il n'y a pas de miracle : elle est fausse.

http://www.zdnet.fr/galerie-image/0,50018840,39706388,00.htm

Paru le 2009-09-16 13:21:00

Espagne - Les cybercriminels profitent de la peur que génère la grippe porcine.

Ces derniers envoient en effet dans les boîtes aux lettres du monde entier des emails promettant des actualités sur la maladie.
La société espagnole Pandasecurity avertit que ces emails invitent l'internaute à ouvrir un document prouvant que le virus H1N1 a été développé par des groupes pharmaceutiques pour réaliser d'immenses bénéfices.
Si l'internaute curieux passe à l'acte et ouvre le document, un virus s'installe sur son ordinateur : ce virus va ensuite essayer de voler des données personnelles, bancaires par exemple.
Le phénomène a même fini par provoquer une question sur ce sujet lors d'une interview de Margaret Chan, qui dirige l'OMS. Cette dernière a répondu qu'elle ne pouvait pas imaginer que les groupes pharmaceutiques soient capables de générer une pandémie, d'autant que l'on sait que ces dernières surviennent régulièrement.
On a estimé qu'environ 2 milliards de gens pourraient être infectés dans le monde par ce virus les deux prochaines années, soit un tiers de la population mondiale.

Les guerriers du web

Les créateurs de virus informatiques sont en mesure de contrôler des millions d'ordinateurs à distance pour créer de puissants réseaux illicites qui servent à de nombreuses activités criminelles. Devenu une véritable arme de guerre, le piratage informatique vise tant les particuliers que les gouvernements et les grandes firmes. Le cyber-espace est devenu un réel champ de bataille.

Les escroqueries sur internet se multiplient et les cyberarnaqueurs se professionnalisent. Désormais, ils utilisent des méthodes marketing pour mieux nous piéger.

Les cyberescrocs sont de vrais professionnels. C'est ce que révèle un rapport publié par Cisco, le fabricant américain de matériel informatique. **Les escroqueries en ligne sont devenues un business comme un autre**. Et les pirates n'hésitent pas à surfer sur l'actualité.

Récemment, ils ont tiré profit de l'émotion causée par le décès de **Michaël Jackson** pour envoyer des milliards de pourriels.
Leur méthode? Susciter la curiosité de leurs victimes potentielles en diffusant de fausses informations sur la mort du roi de la pop.

Autant de e-mails destinés à vous inciter à cliquer sur des liens internet qui vont infecter votre ordinateur de **virus malveillants**. **Une fois installés sur votre machine, ces programmes sont capables de dérober des données confidentielles et de prendre le contrôle de votre ordinateur.**

Et ce n'est pas tout, sur le Net, les pirates font appel aux méthodes éprouvées du marketing traditionnel. Ils inondent leurs **sites piégés** de **mots-clefs** les plus demandés par les internautes dans les moteurs de recherche… Pour mieux vous attirer.

Paru le 2009-09-13 12:31:00

Monde - Les États-Unis et le Brésil continuent à émettre le plus grand nombre de spams et de virus, même si l'on remarque que les niveaux ont diminué depuis juillet dernier.

En août, une analyse des menaces sur Internet par la société *Network Box* a montré que le volume de *malware* a connu un grand pic en juillet (+ 300 %) avant de revenir au niveau enregistré en juin en août dernier.
Les États-Unis sont toujours la principale source de virus dans le monde : 15.9 % des virus proviennent de ce pays. Le Brésil les suit de près, avec 14.5 % et s'impose également comme la principale source de spams (11.6 % devant les États-Unis et la Corée qui ne produisent respectivement que 8.6 % et 7.2 %).
La Corée du Nord reste pour sa part la principale source d'attaques intrusives (17.3 %).

La cybercriminalité a dépassé les revenus du trafic illégal de drogue

Publié le **22/09/2009** Dans Press Releases Par zion

Un crime est commis toutes les trois minutes et demi dans les rues de New York. Un crime est commis toutes les deux minutes et demi dans les rues de Tokyo. Mais toutes les trois secondes, une identité est volée en ligne, soit près de 10 512 000 d'identités chaque année. La cybercriminalité est devenu un crime à part entière, bien plus rentable, avec un meilleur anonymat, et peut s'avérer beaucoup plus difficile à poursuivre que les crimes réels.

VOIR

http://www.dailymotion.com/video/x7krty_securite-internet-la-securite-sur-i_tech

http://www.dailymotion.pl/video/x9stko_pirater-une-carte-bleue_lifestyle?from=rss

http://www.dailymotion.com/video/xak6r5_arte-reportage-hackers-wifi_tech

http://www.secuser.com/

http://www.securite-informatique.gouv.fr/

http://www.zataz.com/

http://assiste.com.free.fr/

Les PANNES

Par Bouarfa Mahi le 1 août 2005
http://www.gpcservices.com/bouarfa_mahi/2006/12/depannage-informatique-a-domic-3.html

La panne informatique est inhérente au système d'exploitation Windows. La raison en est très simple : un ordinateur est essentiellement assemblé à partir de pièces standards réalisées par différents fabricants, des problèmes de compatibilité et/ou d'instabilité peuvent apparaître à moyen terme lors de son utilisation. Ainsi les vendeurs proposent toujours des correctifs logiciels pendant la durée de vie de l'ordinateur. Ces correctifs apportent une meilleure compatibilité entre le matériel et le système Windows. C'est cette multitude d'acteurs dans le domaine matériel qui rend difficile une compatibilité à 100 %. On dira que le monde PC est un système ouvert.
Lors de notre étude expérimentale réalisée d'octobre 1998 à mars 2000 et portant sur 300 interventions, nous avons trouvé que **les pannes sont en majorité (98%) de nature logicielle**.

Le très faible taux de pannes matérielles est lié à une excellente qualité de fabrication des composants entrant dans la fabrication et l'assemblage d'un ordinateur.
Il n'est pas étonnant de constater que le gros de la troupe soit 68.26% concerne Windows et les applications ; windows car c'est le moteur de l'ordinateur et les applications car elles sont utilisées couramment pour effectuer les tâches bureautiques et internet.

Ensuite dans la même proportion soit 15.73% nous avons les problèmes liés d'une part à l'installation de pilotes et d'autre part aux dysfonctionnements dus à la présence de virus et de spywares pouvant amener à considérer la restauration du système dans les cas les plus graves. Ce qui ne veut pas dire que l'on ne trouvera pas de problèmes liés à des virus dans la partie des 68.26%.

Les SOLUTIONS Jean-Pierre Louvet

http://www.futura-sciences.com/fr/doc/t/informatique-2/d/proteger-son-ordinateur-conseils-et-astuces_627/c3/221/p1/

Pare-feu, ou firewall

Le pare-feu est la première protection indispensable de tout ordinateur relié à l'Internet. Son rôle est de bloquer les tentatives d'intrusion dans l'ordinateur par un pirate ou un virus. Il doit bloquer aussi toute tentative de connexion non autorisée à l'Internet par un programme résident sur l'ordinateur (par exemple un spyware : programme espion). Vous ne devez donc jamais vous connecter à Internet sans pare-feu.

Mise à jour du système

Les mises à jour du système d'exploitation sont destinées à corriger des bugs et des failles de sécurité. Votre système doit donc impérativement être à jour. En particulier le Service Pack 2 doit être installé car il comble des failles graves et, sauf exception rarissime, il n'y a pas de bonnes raisons pour l'écarter. Pour Windows les mises à jour sont publiées le deuxième mardi (heure US) de chaque mois.

Utilisation d'un compte à droits limités

Dans les versions de Windows à base NT (2000, XP) il est possible de limiter les droits octroyés aux différents utilisateurs. Le problème est que par défaut la session est habituellement ouverte en mode administrateur (c'est le mode qui peut tout faire) ce qui fait qu'un malware s'introduisant dans l'ordinateur héritera lui aussi des droits de l'administrateur. **Une règle de base de la sécurité est de ne jamais ouvrir de session en mode administrateur, sauf pendant le bref temps nécessaire pour effectuer certaines opérations (installer un programme, gérer le système...).** De plus l'accès au compte administrateur doit être protégé par un mot de passe robuste (7 à 8 caractères en mélangeant plusieurs types de caractères : majuscules, minuscules, chiffres et signes de ponctuation).

Antivirus

Il existe d'excellents antivirus gratuits : on peut citer par exemple Antivir, Avast ou AVG. Vous devez impérativement régler l'antivirus pour qu'il aille chercher **quotidiennement** sur le site de l'éditeur la présence de mises à jour. Divers spécialistes de la lutte contre les infections affichent actuellement une préférence pour Antivir en raison d'une excellente rapidité de mise à jour lors de l'apparition de nouveaux malwares.

Antispywares

Ces programmes suppriment les programmes espions et peuvent éventuellement avoir des rôles plus étendus. Deux programme gratuits peuvent être recommandés : **Adaware SE et Spybot Search and Destroy**. Ces deux programmes utilisent des techniques d'exploration différentes et peuvent donc être complémentaires. Comme les antivirus ils utilisent une base de données qui doit être mise à jour régulièrement. Un scan hebdomadaire de l'ordinateur est recommandé.

Vaccination et blocage de l'accès à certains sites

La vaccination est une opération qui consiste (pour l'essentiel) à modifier la base de registre de façon à bloquer l'installation (ou s'ils sont déjà présents sur l'ordinateur, l'activation) de nombreux malwares, spécialement ceux qui utilisent la technique ActiveX.
Spybot possède une fonction de vaccination.

Autre programme de désinfection utile

AVG Anti-Spyware (anciennement Ewido) est un programme qui est consacré aux spywares, hijackers, vers, dialers, chevaux de Troie et keyloggers. Il semble avoir une très bonne réputation d'efficacité. La version téléchargée a toutes les fonctionnalités pendant deux semaines.
Au bout de ce délai la surveillance en temps réel et la mise à jour automatique sont désactivées si vous n'avez pas acheté le programme, mais il est toujours possible de faire les mises à jour manuellement et de se servir du programme pour scanner l'ordinateur.

Utiliser Internet avec des programmes plus sûrs

Internet Explorer et Outlook Express sont les programmes les plus visés par les créateurs de malwares. En outre ils incorporent la technologie ActiveX qui les rend potentiellement vulnérables. **Vous améliorerez grandement votre sécurité en utilisant comme navigateur Firefox ou Opera, et Thunderbird comme programme de courrier.**

Ayez un comportement prudent

Un adage de la sécurité informatique est que la faille principale du système se trouve entre le clavier et la chaise. **Ceci signifie que vous éviterez à peu près tous les ennuis en adoptant un comportement raisonnable.**
La plupart des vers ou virus arrivent par mail : utilisez donc toujours la dernière version de votre programme de mail, corrigée des failles connues. N'ouvrez jamais les pièces jointes et ne cliquez jamais sur un lien d'un message dont vous ne connaissez pas l'expéditeur. Même si vous connaissez l'expéditeur, assurez-vous bien que l'envoi de cette pièce jointe est plausible : votre correspondant a pu se faire infecter à son insu, ou bien ce peut être une usurpation d'identité (le plus classique actuellement).

D'autres programmes nocifs peuvent arriver par messagerie instantanée ou se trouver sous des noms très attractifs, mais fallacieux, dans des ordinateurs offrant des fichiers en P2P. **N'oubliez pas, comme cela a été dit plus haut, que tout nouveau fichier arrivant sur votre ordinateur doit être scanné par votre antivirus, même si c'est un document Word, une archive .zip, ou une image.**

Certains malwares peuvent contaminer l'ordinateur simplement par l'ouverture d'une page ou d'une image piégées. Même si vous avez appliqué les mesures de sécurité ci-dessus, évitez les sites qui vous semblent plutôt « border line » par exemple par leur contenu photographique ou par la mise à disposition en téléchargement de programmes qui ne devraient se trouver que dans le circuit commercial.

Le dernier conseil concerne plutôt votre propre protection : évitez le phishing. Votre banque, compagnie d'assurance, service de paiement en ligne… ne vous contacteront jamais par mail pour vous demander vos mots de passe, vos coordonnées de carte bancaires, même si ces message vous paraissent bien imités et vous offrent de cliquer sur un lien qui semble être de celui de la banque, par exemple. Ce sont en réalité des sites imités pour vous mettre en confiance et pour vous soutirer des informations qui serviront à exploiter vos comptes à votre insu.

Je suis pressé ! Pas le temps de lire !
http://assiste.com.free.fr/p/kit_securite/kit_securite.html
Pour ceux qui ne savent pas lire, qui n'ont pas le temps de réfléchir, et pour les nuls, voici ce qui se fait de mieux : on sort sa carte bancaire et on boucle le problème avec la collection des outils les plus solides dans chaque compartiment, que la machine soit à usage professionnel ou personnel. Installez ce qui suit en 5 minutes chrono !

Navigation - Gratuit Firefox Messagerie - Gratuit Thunderbird Antivirus KAV Kaspersky Antivirus
Anti-trojans / Anti-spywares AVG Anti-Spyware
Protection périmètrique - Pare-feu Outpost Pro
Protection périmètrique - Risques majeurs Zeb Protect
Anti-spam Pro : MailInBlack ou Gratuit et personnel : SpamPal
Proxy-local Spyblocker
Anti-ActiveX hostiles - préventif - gratuit SpywareBlaster
Anti-spyware - préventif - gratuit SpywareGuard
Boîte à outils - gratuit Spybot Search & Destroy
Contrôle d'intégrité - préventif ProcessGuard
Anti-failles proactif - préventif Qwik Fix
Nettoyeur de traces internes - gratuit CCleaner
Nettoyeur de traces internes - gratuit ATF Cleaner
Nettoyeur de traces internes - gratuit MRUs Blaster
Durcissement gratuit 1 XP-Antispy Durcissement gratuit 2 Safe XP Réglages préventifs divers - gratuit : partie préventive de La Manip

Avec cela, vous êtes tranquille - votre machine est bétonnée et, selon l'expression de Vazkor sur nos forums, elle ressemblera à un "sous-marin nucléaire d'attaque en plongée profonde en temps de guerre".

Il existe une solution plus simple à mettre en oeuvre que l'utilisation de ces ensembles d'outils

Une solution qui ne vous empechera pas de cotoyer virus, malware, spyware et autres...mais dont il ne restera STRICTEMENT AUCUNE TRACE dés l'arrêt de votre ordinateur.

- PRINCIPES (**Returnil Virtual System**) Pour Windows **XP** / Windows **Vista** / Windows **7**

Returnil Virtual System Personal Edition est un programme qui protège votre système des nombreuses modifications qui peuvent intervenir sur la machine. Quelles soient d'origine malveillante ou simplement de mauvaises manipulations.

Returnil créé une copie de votre système à chaque démarrage, vous n'utilisez plus le système mais une copie, dès lors tous changements effectués seront inexistants après redémarrage puisque il rechargera de nouveau une copie de votre système.
Ceci peut être très interressant pour tester des programmes ou surfer de manière sécurisée (en cas d'infection aucun risque pour votre machine puisque l'infection aura eu lieu sur la copie du sytème).

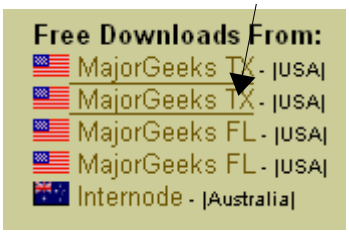
Gratuit pour une utilisation personelle, c'est le MUST en termes de maintenance préventive.
Vous réduisez de 90%, les risques de pannes de votre ordinateur.

3- INSTALLATION

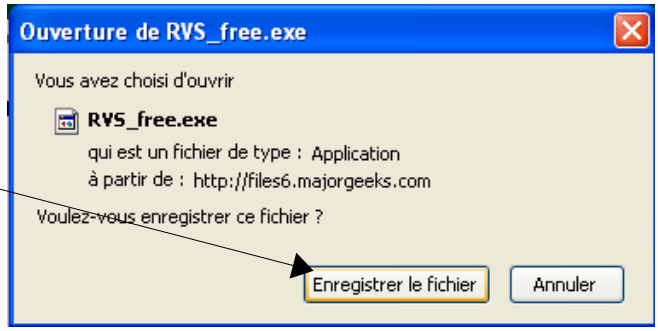
Téléchargez le programme à cette adresse
http://www.returnilvirtualsystem.com/index_files/rvspersonal.htm

Cliquez sur 

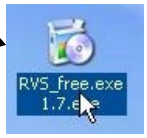
Puis sur l'un des liens de téléchargement



Enregistrez le fichier

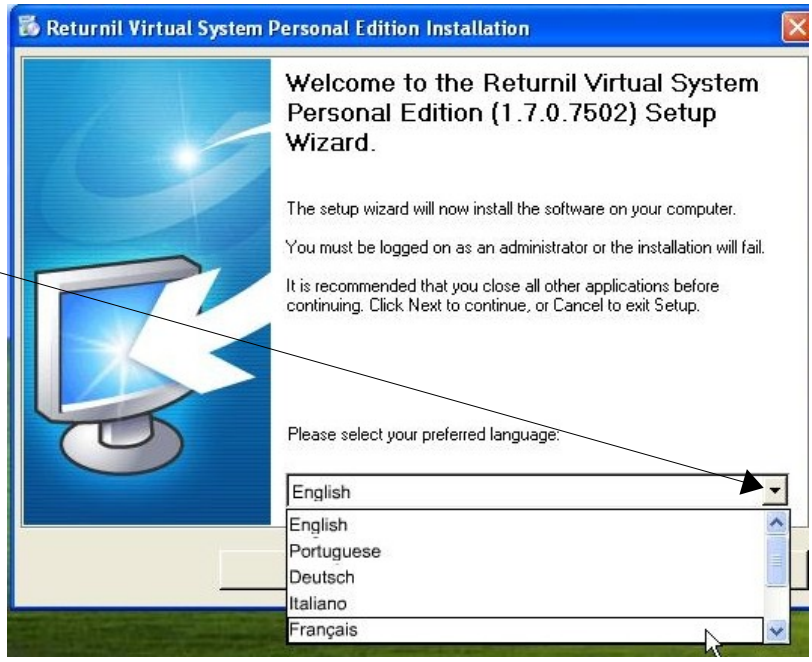


2 clics sur le fichier téléchargé pour procéder à l'installation



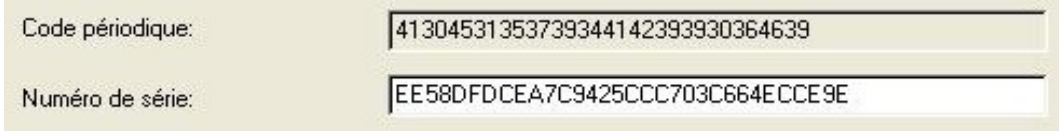
La procédure démarre; sélectionner la langue Française
puis

Ensuite Accord de Licence



Répertoire d'installation, vous ne touchez à rien

Le numéro de série s'inscrit automatiquement (gratuit)



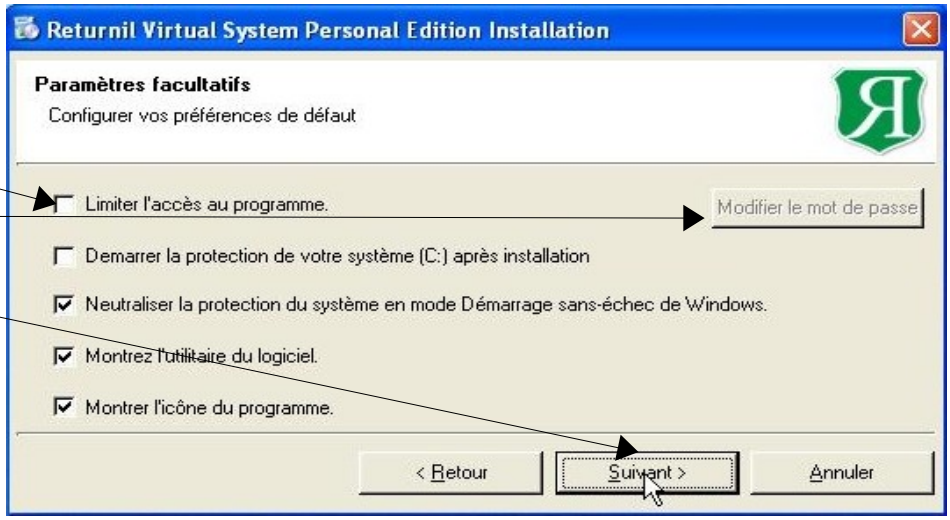
Suivant

Si je souhaite protéger l'accès au programme par un mot de passe, je sélectionne l'option et j'irai ensuite saisir le mot de passe

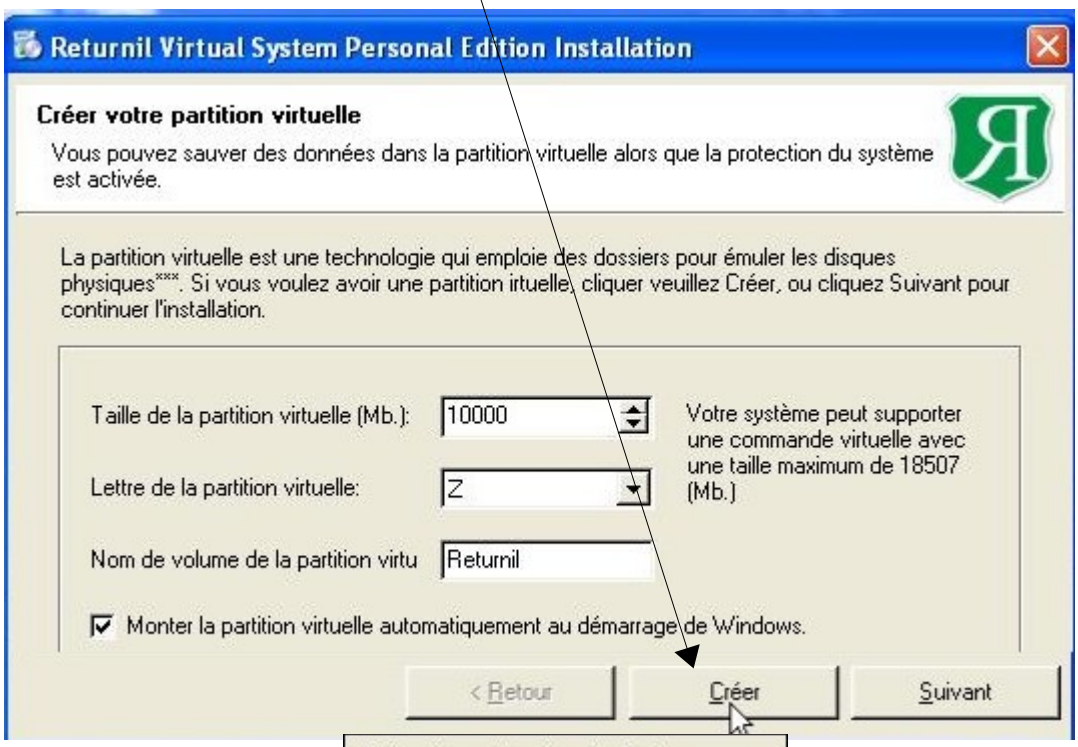
Je clique sur suivant

et ensuite

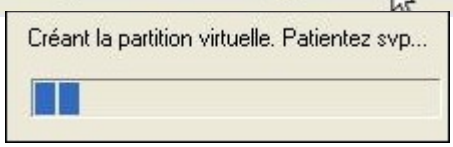
Progression de l'installation



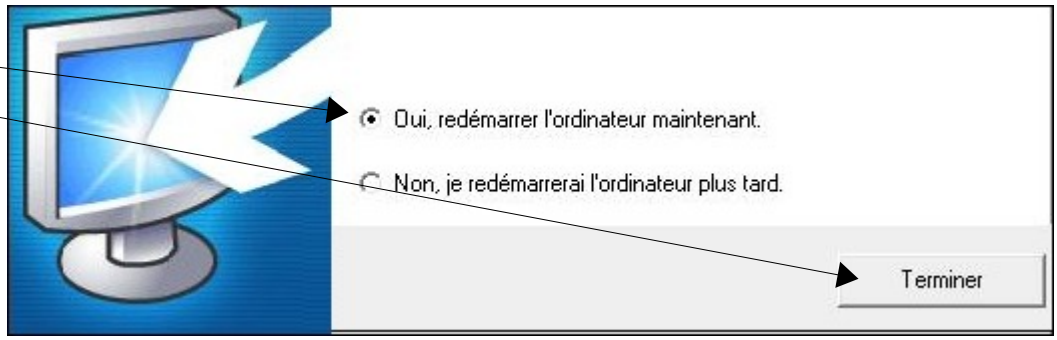
IMPORTANT: Dans cette étape il nous est proposé de Créer une partition virtuelle.
Je suis informé de la taille maxi possible. Dans cet exemple j'ai choisi de créer une partition de 10000 Méga (soit 10 Giga). Il vous faut IMPERATIVEMENT créer cette partition virtuelle (explication plus loin)



La procédure peut être longue, soyez patient



Ensuite
Terminer



4- CONFIGURATION

Aprés le redémarrage, Rvs apparait dans les programmes résidents dans la barre des tâchesà coté de l'heure

Dans le poste de travail je constate la partition virtuelle RETURNIL (Z:),(C:) représente la partition système.

Nous avons dit qu'avec RVS, le système redémarre à l'identique.
Or, si je souhaite réaliser ou enregistrer des documents cela ne peut pas se faire sur C: puisque il est protégé. La partition RETURNIL va nous permettre de pouvoir faire cela simplement.

Nous souhaitons pour des raisons d'ordre,organiser SYSTEMATIQUEMENT l'enregistrement de nos documents dans le dossier **Mes documents.** Regardons de plus près ses propiétés...

Clic Droit sur mes documents et clic sur propriétés
Pour l'instant le dossier Mes documents est sur C:
Nous allons le déplacer de façon à ce que son contenu aille vers la partition RETURNIL

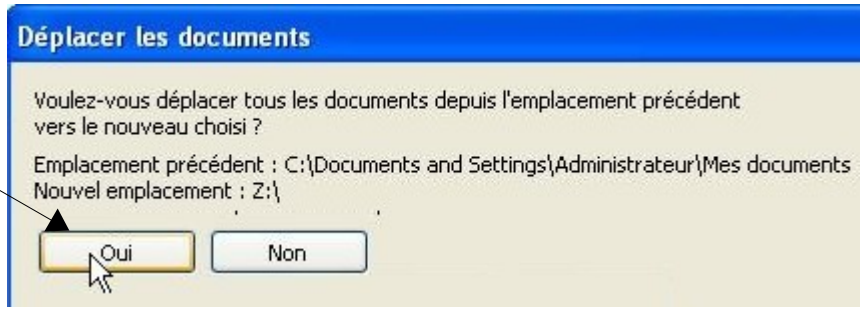
Je sélectionne la destination (partition ”Returnil”) en cliquant sur le Poste de travail

Puis je sélectionne **RETURNIL** et je confirme

Lisez

Ne reste qu'appliquer et OK

CONFIRMER



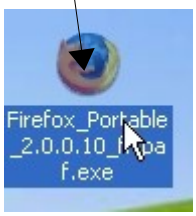
AUTRE CHOSE

Quand nous naviguons sur Internet, nous souhaitons pouvoir ajouter dans nos favoris, des pages web sur lesquelles nous souhaitons revenir rapidement. Avec le navigateur Internet Explorer je n'ai pas trouvé de solutions qui permettent de faire évoluer au grés de vos envies les favoris. MAIS....
cela est possible avec le meilleur des naviguateur (issu du monde des logiciels libres) Firefox.
Vous savez naviguer avec Internet explorer, vous apprécierez rapidement Firefox.

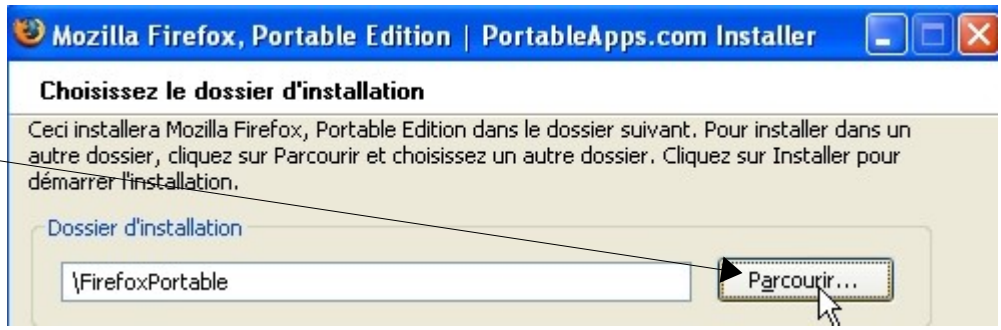
La version qui nous conviendra est la version **Firefox Portabe**. Allez à l'adresse/
http://portableapps.com/apps/internet/firefox_portable/localization
et cliquez sur French Download

Language		Version	Link
English	English	2.0.0.10	Homepage
French	Français	2.0.0.10	Download*
German	Deutsch	2.0.0.10	Homepage
Italian	Italiano	2.0.0.10	Download*

Enregistrez le fichier sur votre ordinateur
et double cliquez dessus pour exécuter l'installation.



Suivez logiquement la procédure jusqu'à cette fenêtre.
Le dossier d'installation devra se trouver sur la partition RETURNIL
Cliquez donc sur **Parcourir** et suivez la même procédure que à la fin de la page 5 (poste de travail/RETURNIL et OK)

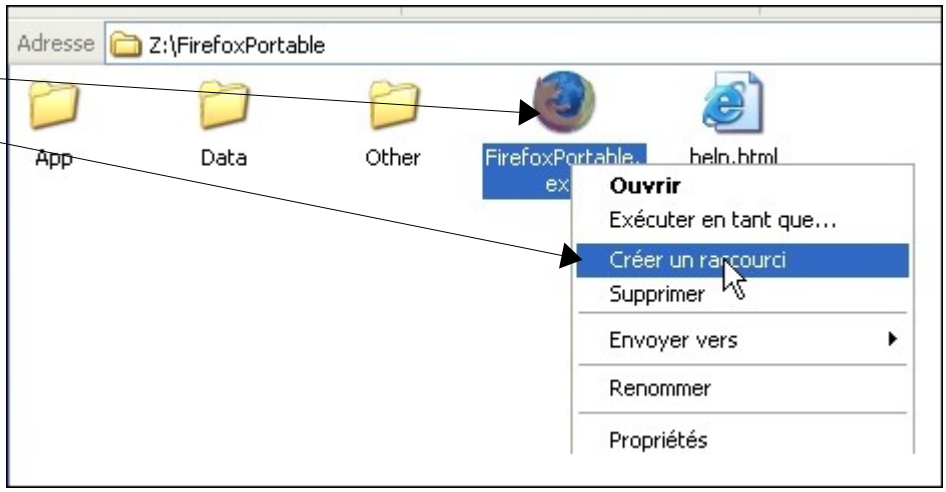


Fin de la procédure.....

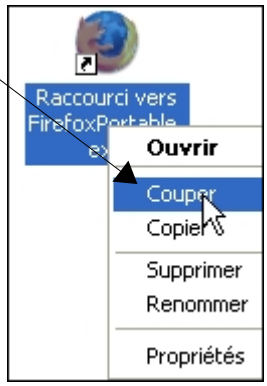
Ne nous reste qu'a créer un raccourcis qui nous permettra de lancer Firefox à partir du bureau.

J'ouvre le dossier FirefoxPortable qui se trouve dans le dossier Mes documents

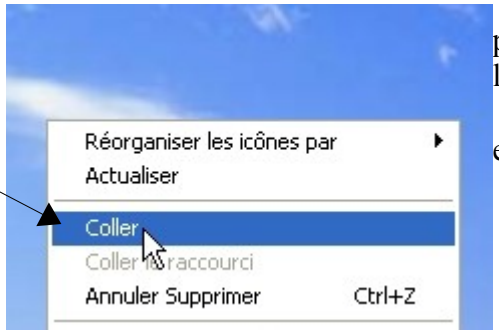
et je fais un Clic Droit sur l'exécutable puis je clique sur



Je coupe ensuite ce raccourcis



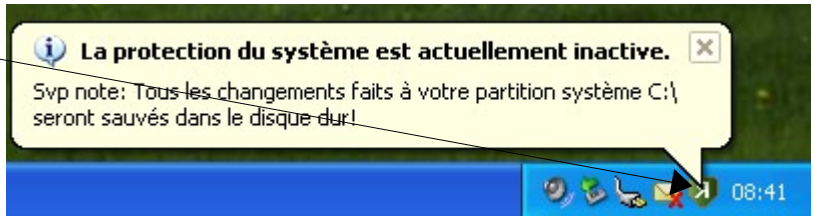
pour le coller sur bureau

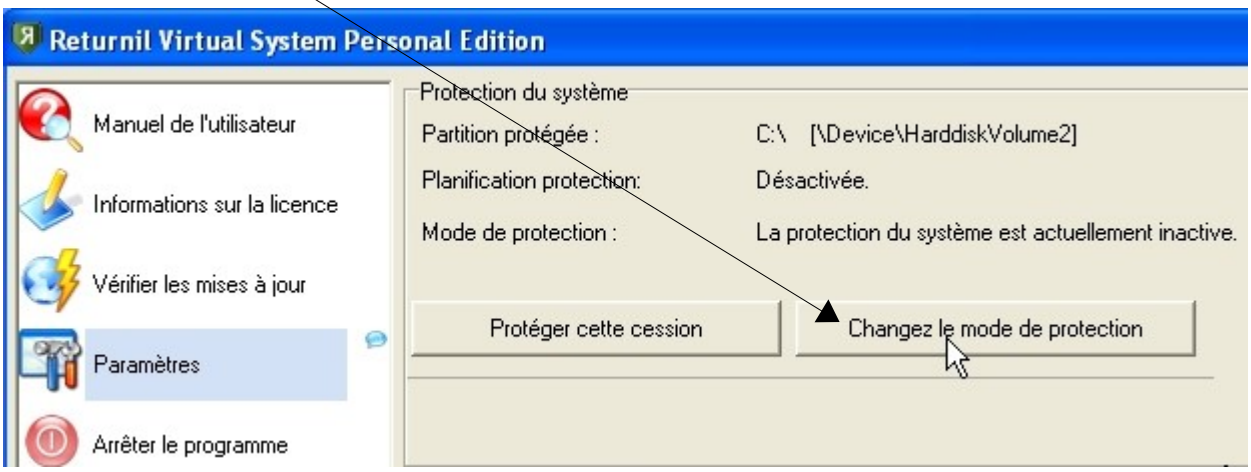


et voilà

Si vous utlisez un gestionnaire de messagerie tel que Outlook express, il vous sera possible de le faire avec **Thunderbird portable** que vous trouverez ici:http://www.framakey.org/Portables/PortableThunderbird
Même procédure que avec Firefox.

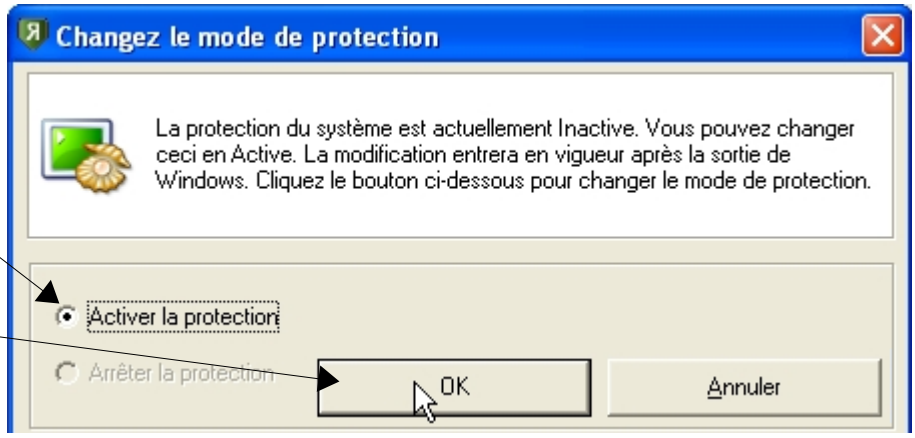
Nous avons préparé notre ordinateur pour l'utiliser à notre convenance.
Il suffit maintenant **d'activer la protection de Returnil Virtual System** pour être DEFINITIVEMENT tranquille.
Quand **RVS est vert**, la protection **n'est pas active**.Je clique donc 2 fois sur l'îcone qui le représente pour Changer le mode de protection





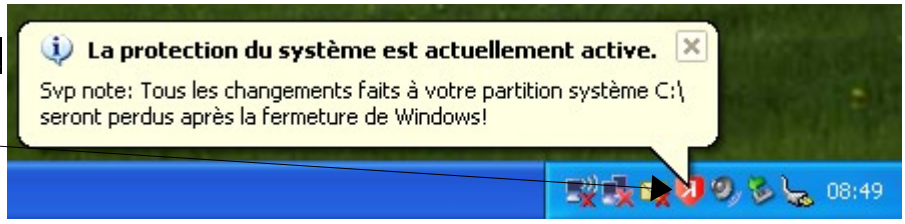
Je sélectionne Activer la protection

et je confirme



Lisez

Au redémarrage la protection est en rouge, vous êtes protégés.



Votre ordinateur est définitivement protégé contre toutes mauvaise manipulation ou programme malveillant quelqu'il soit. Si vous aviez durant l'utilisation quelques soucis que ce soient il suffira de le redémarrer pour le retrouver NICKEL. Vous aurez compris que ce programme s'installe sur une machine **Propre.**
Si vous souhaitez apporter une modification à votre machine (installer un programme, installer une imprimante, faire des mises à jour...) il faudra d'abord désactiver la protection pour la réactiver aprés les modifications.