

Maintenance Préventive

1- POURQUOI

Le surf sur [Internet](#) nous expose à des attaques venant de toute part (liens piégés, sites frauduleux etc...). Parfois, ces attaques aboutissent et infectent nos [ordinateurs](#), malgré les protections déjà en place. Certains symptômes apparaissent alors, nous laissant penser que notre machine est infectée.

Ce peut être des fenêtres publicitaires surgissant de façon intempestives sur votre bureau, des [icônes](#) se rajoutant sans votre consentement dans la barre des tâches, vous alertant d'une hypothétique infection et vous proposant l'achat de telle ou telle solution miracle, ou encore le détournement de votre fond d'écran, là aussi en vous alertant d'une infection. Dans d'autres cas les symptômes sont plus discrets et se traduisent par un ralentissement de l'ordinateur, une activité anormale du [disque dur](#) ou d'autres comportements étranges.

Tous ces symptômes doivent vous alerter, sans pour autant vous paniquer. En effet, une infection n'attaque que très rarement vos données personnelles, et le formatage n'est qu'une solution de tout dernier recours. Toutefois, dans la plupart des cas, les solutions classiques (antivirus, antispywares...) sont incapables d'éradiquer totalement l'infection, même si ces outils sont très utiles pour la prévention.

Les [malwares](#) ont en effet fait de tels progrès – et évoluent tellement vite – que leur éradication ne peut être faite que par des personnes au courant des dernières évolutions dans ce domaine.

L'usage de certains outils de diagnostic peut se révéler dangereuse pour l'ordinateur si vous ne respectez pas la procédure.



Il faut attirer l'attention sur le fait qu'à côté des désagréments visibles rencontrés par les utilisateurs il y en a d'autres, non visibles mais beaucoup plus graves. Certains programmes infectieux peuvent espionner vos frappes au clavier et envoyer à un pirate votre numéro de carte bancaire, vos mots de passe sur des sites d'achat, etc. D'autres transforment à votre insu l'ordinateur en machine à envoyer vers des adresses diverses des milliers de [spams](#), ou se servent de lui comme arme pour attaquer des sites commerciaux ou institutionnels.

Protégez gratuitement votre PC sous Windows

De l'antivirus au pare-feu, en passant par le nettoyage ou le renforcement du système, il n'y a plus d'excuse pour ne pas "blinder" son PC. Notre sélection d'outils gratuits.

LES PRODUITS ESSENTIELS :

1. Les antivirus

· [Antivir](#) : efficace, léger et souvent mis à jour. Le débat de sa supériorité face à [avast!](#), l'autre antivirus gratuit majeur, est sans fin. Nous avons toutefois choisi de préférer Antivir.

2. Le pare-feu

Pour les utilisateurs néophytes, le pare-feu intégré à Windows suffit largement. Il faut cependant s'assurer qu'il est bien activé (ce qui est le cas par défaut sous Windows XP SP2), et penser à supprimer les exceptions qu'il octroie automatiquement à certains programmes.

3. Les antispywares

De très nombreux produits se disputent ce créneau à la mode, mais peu ont fait leurs preuves parmi les gratuits. Parmi notre sélection, vous pourrez tous les essayer, car contrairement aux antivirus, cela ne fait pas de mal d'avoir plusieurs anti-spywares sur son PC. Attention cependant : n'activez la protection en temps réel que d'un seul produit en même temps.

· [AdAware](#) : l'un des plus anciens et des mieux connus.

· [Spybot Search & Destroy](#) : l'autre grand nom historique du domaine. Plus rustique que AdAware, mais pas moins efficace. Propose une protection en temps réel.

4. Nettoyer en profondeur son PC

· [CCleaner](#) : l'outil idéal pour débarrasser le système de l'inutile et de l'encombrant (fichiers temporaires, etc.). Cela ne vous protégera pas contre les intrusions, mais un système propre est bien plus stable.

LES OUTILS POUR EXPERTS :

1. Un vrai pare-feu

· [Outpost Free](#) : un excellent pare-feu gratuit, particulièrement complet. Le néophyte sera cependant probablement perdu face aux options de configuration

2. Restreindre les droits

· [Drop My Rights](#) : si comme le reste de la planète vous utilisez Windows XP en tant qu'administrateur (ce qui est hélas souvent indispensable), cet outil gratuit livré par Microsoft est incontournable. Il permet de rester administrateur pour la plupart des applications tout en exécutant certaines d'entre elles avec des droits limités.

3. Maîtriser le navigateur

· [NoScripts](#) : réservé aux utilisateurs de Firefox, cette extension permet de limiter l'usage des scripts aux seuls sites de confiance, et de bloquer par défaut tous les autres. Une saine approche de la sécurité !

4. Détecter les modifications

· [WinPatrol Free](#) : l'outil indispensable pour les utilisateurs avancés. WinPatrol surveille de nombreux points-clés du système (base de registre, fichiers de configuration, etc.) essentiels à la survie des codes malveillants, et il donne l'alerte en cas de modification. La version gratuite procède à un contrôle régulier (toutes les minutes, par exemple). WinPatrol est un outil très efficace pour qui comprend que la modification soudaine du fichier hosts est rarement une bonne nouvelle. Les autres passeront probablement à côté de ses trésors.

5. Connaître l'état du système

· [HijackThis !](#) : un utilitaire bien connu des traqueurs de virus et autres spywares, HijackThis! permet de collecter des informations essentielles à propos de l'état du système. HijackThis se contente de livrer un rapport très complet, qu'un expert saura analyser afin d'y déceler les traces d'une infection éventuelle. L'avantage : il est ainsi possible de détecter des parasites inconnus. L'inconvénient : si vous n'êtes ni expert ni passionné, la lecture d'un rapport d'HijackThis! ne vous apprendra probablement rien et vous donnera certainement mal à la tête !

6. Les anti-rootkits

L'utilisation d'un anti-rootkit est réservé aux amateurs éclairés, non pas à cause d'une quelconque difficulté d'utilisation, mais parce que l'interprétation de ses résultats peut prêter à confusion.

· [AVG Antirootkit](#)

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

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

2- PRINCIPES (Returnil Virtual System) Pour Windows XP et Vista

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 crée une copie de votre système à chaque démarrage, vous n'utilisez plus le système mais une copie, dès lors tous changements effectués seront inexistantes après redémarrage puisque il rechargera de nouveau une copie de votre système.

Ceci peut être très intéressant 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 système).

Gratuit pour une utilisation personnelle, c'est le MUST en termes de maintenance préventive.

Vous réduisez de 90%, les risques de pannes de votre ordinateur.

3- INSTALLATION

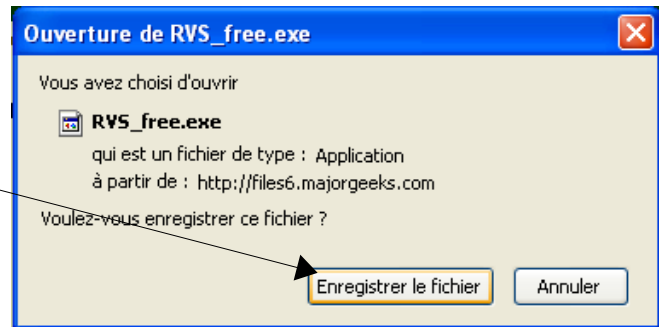
Téléchargez le programme à cette adresse
http://www.returnilvirtualsystem.com/index_files/rvspersonal.htm

Cliquez sur 

Puis sur l'un des liens de téléchargement



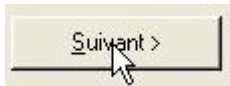
Enregistrez le fichier



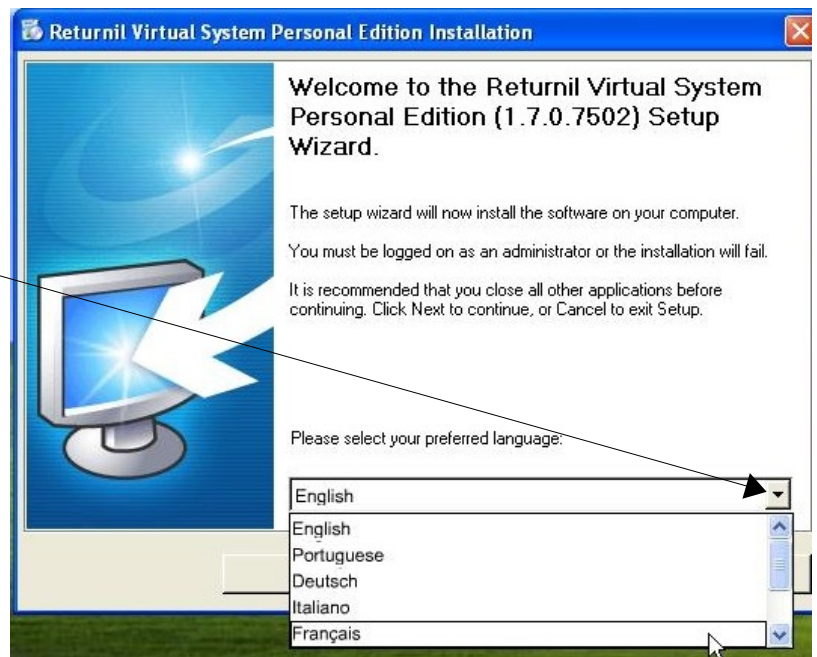
2 clics sur le fichier téléchargé pour procéder à l'installation



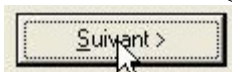
La procédure démarre; sélectionner la langue Française



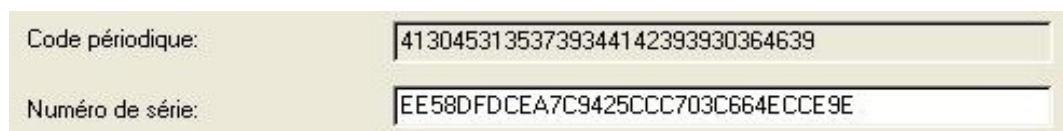
Ensuite Accord de Licence



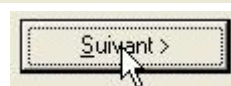
Répertoire d'installation, vous ne touchez à rien



Le numéro de série s'inscrit automatiquement (gratuit)



Suivant



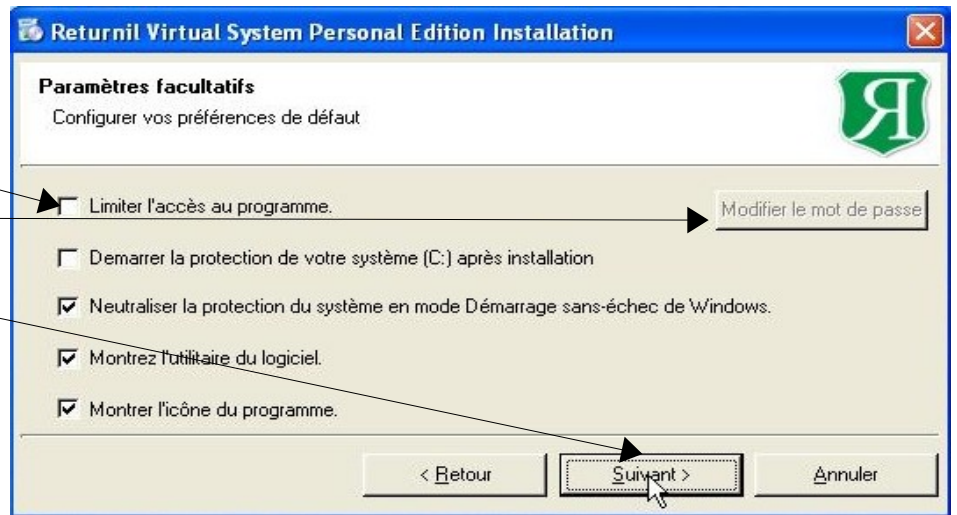
Si je souhaite protéger l'accès au programme par un mot de passe, je sélectionne l'option et j'irai ensuite saisir le mot de passe

Je clique sur suivant

et ensuite

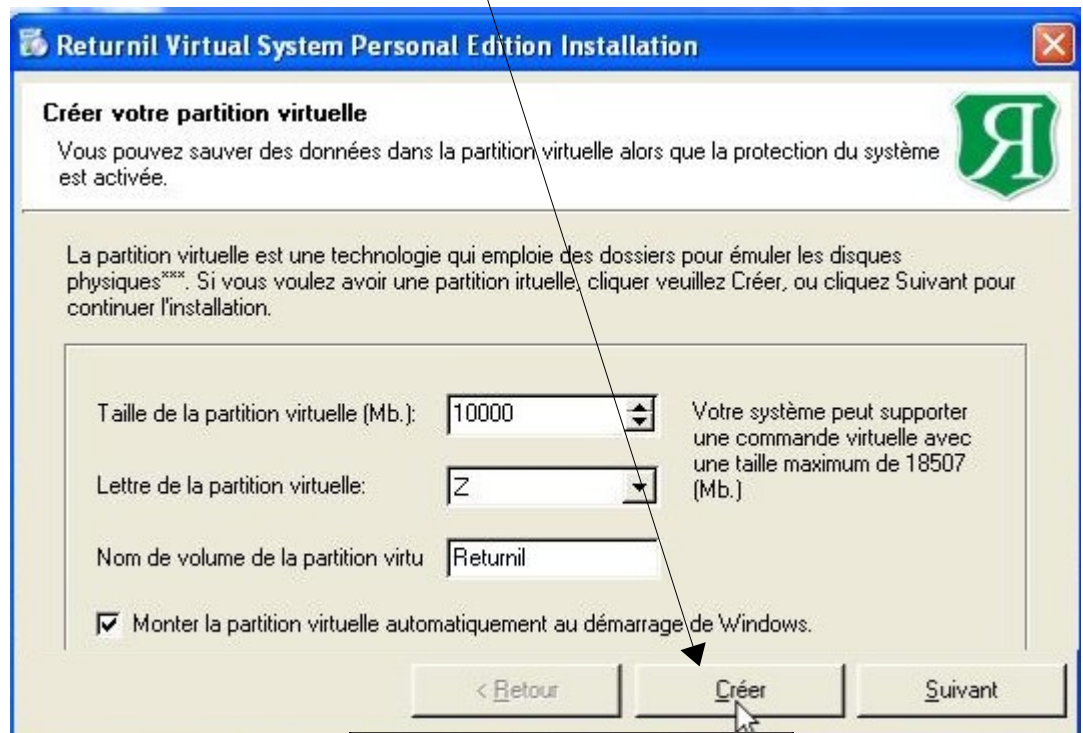


Progression de l'installation

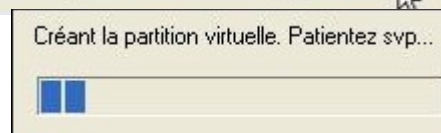


IMPORTANT: Dans cette étape il nous est proposé de Créer une partition virtuelle.

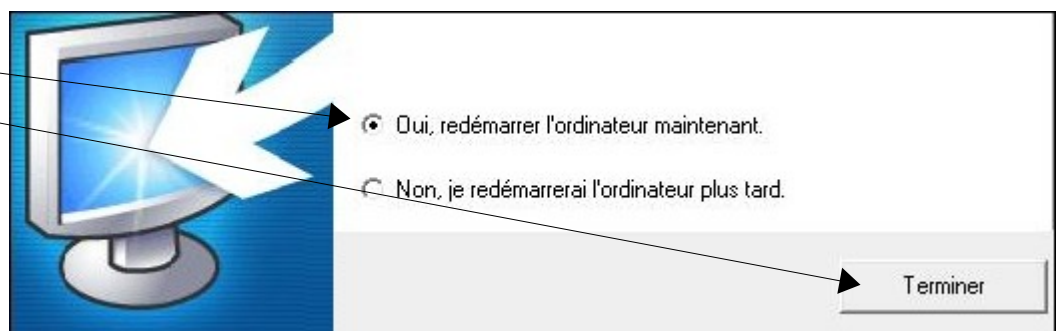
Je suis informé de la taille maxi possible. Dans cet exemple j'ai choisi de créer une partition de 10000 Méga (soit 10 Giga). Il vous faut **IMPERATIVEMENT** créer cette partition virtuelle (explication plus loin)



La procédure peut être longue, soyez patient



Ensuite
Terminer



4- CONFIGURATION

Après le redémarrage, Rvs apparait dans les programmes résidents dans la barre des tâches à côté 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 propriétés...

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



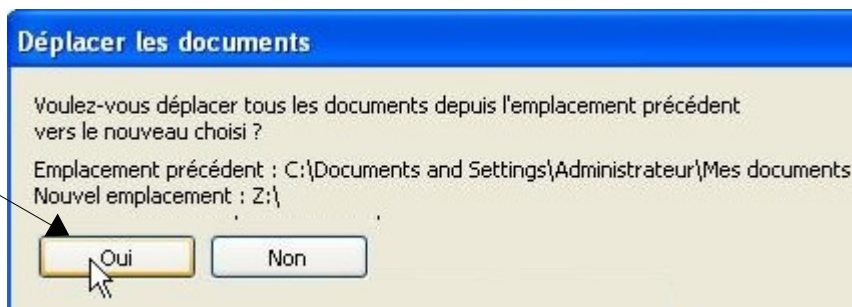
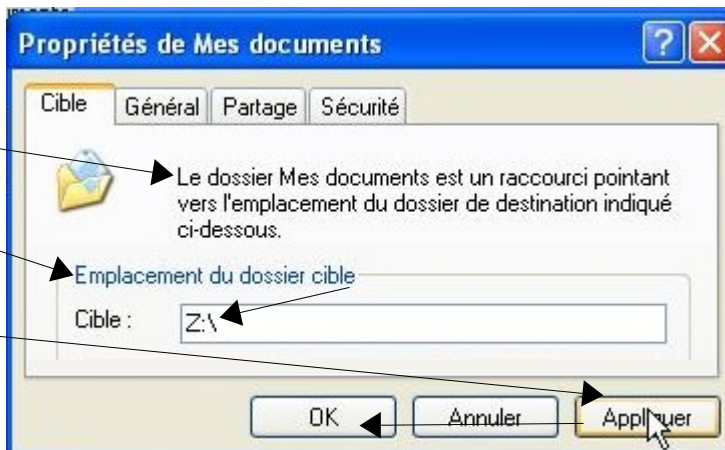
Puis je sélectionne **RETURNIL** et je confirme



Lisez

Ne reste qu'appliquer et OK

CONFIRMER



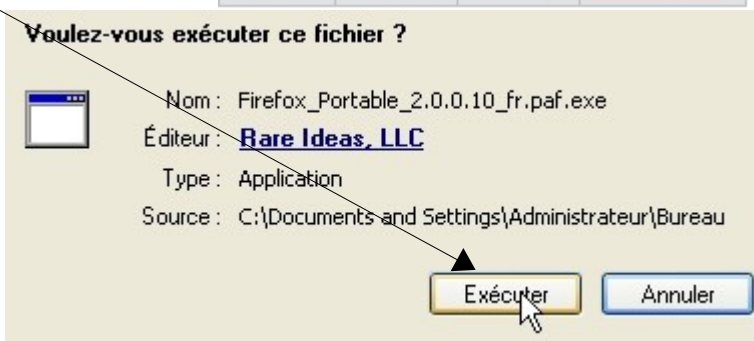
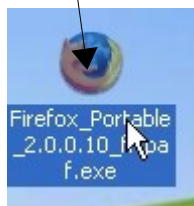
AUTRE CHOSE

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 navigateur (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 Portable**. Allez à l'adresse/ http://portableapps.com/apps/internet/firefox_portable/localization et cliquez sur French Download

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

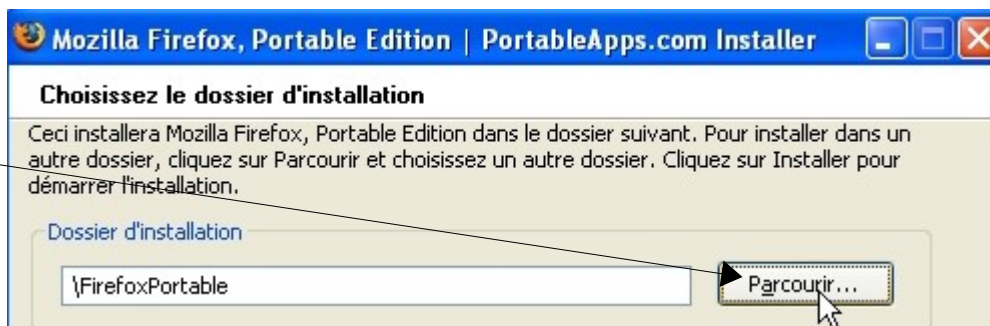
Language	Version	Link
English	English	2.0.0.10 Homepage
French	Français	2.0.0.10 Download*
German	Deutsch	2.0.0.10 Homepage
Italian	Italiano	2.0.0.10 Download*



Suivez logiquement la procédure jusqu'à cette fenêtre.

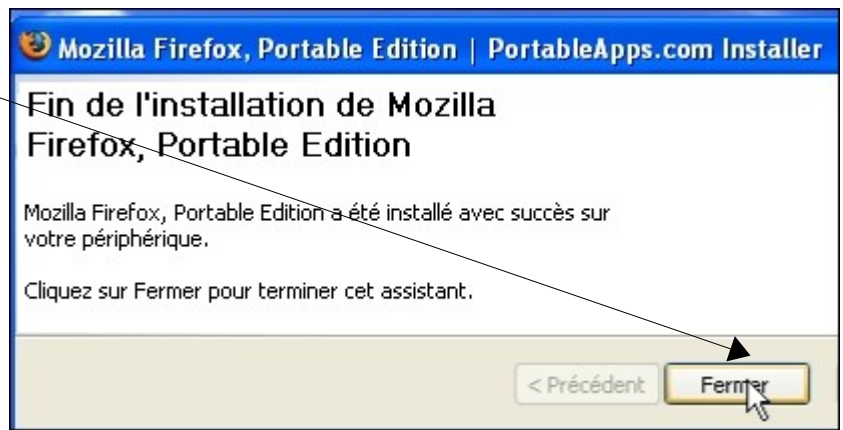
Le dossier d'installation devra se trouver sur la partition RETURNIL

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'à créer un raccourci qui nous permettra de lancer Firefox à partir du bureau.



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

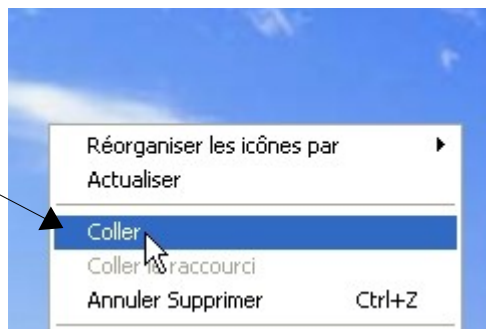
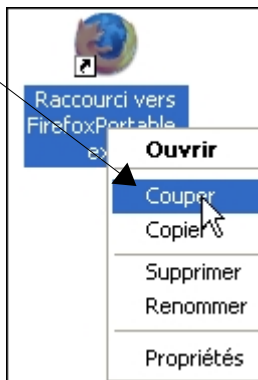
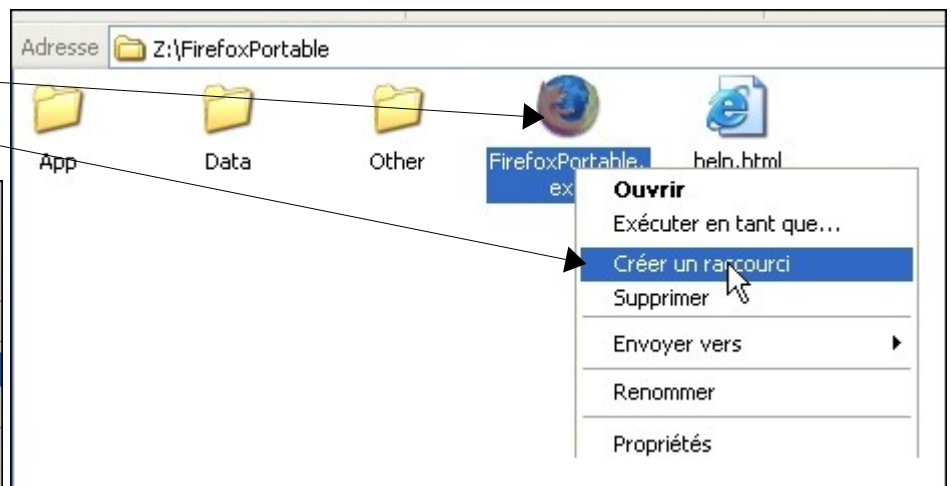


et je fais un Clic Droit sur l'exécutable puis je clique sur

Je coupe ensuite ce raccourci

pour le coller sur bureau

et voilà



Si vous utilisez 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.

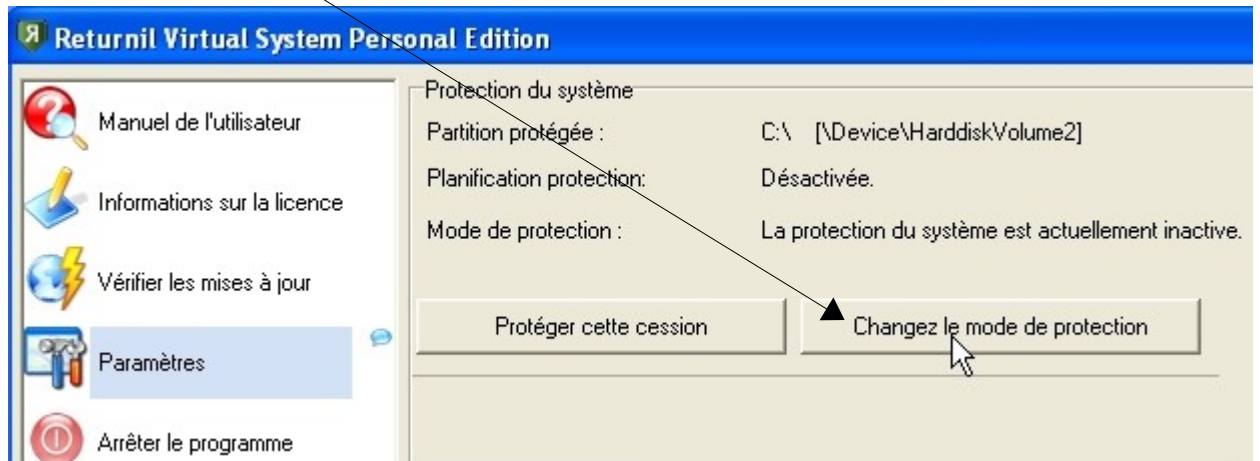
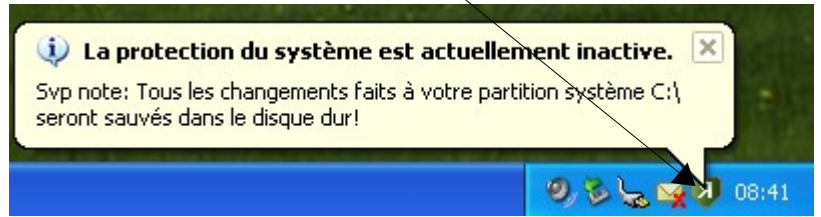
thierry.barbero@laposte.net

www.cyberbases64.canalblog.com

Nous avons préparé notre ordinateur pour l'utiliser à notre convenance.

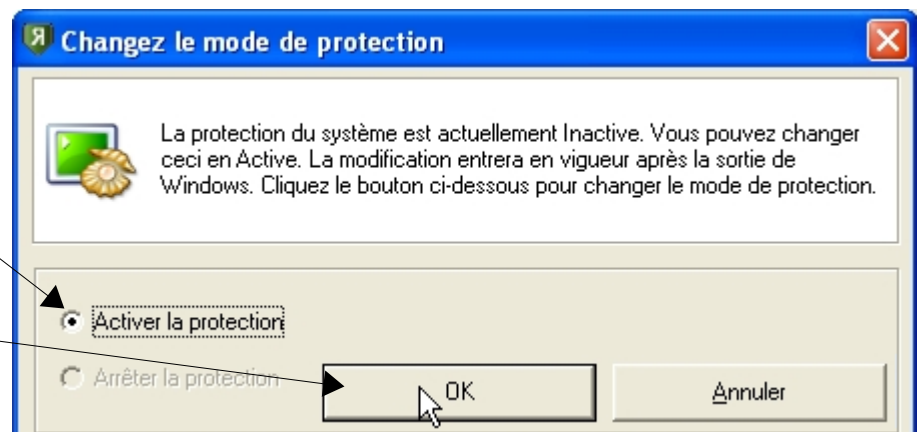
Il suffit maintenant d'activer la protection de Returnil Virtual System pour être DEFINITIVEMENT tranquille.

Quand RVS est vert, la protection n'est pas active. Je clique donc 2 fois sur l'icône 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 quelques modifications à votre machine (installer un programme, faire des mises à jour...) il faudra d'abord désactiver la protection pour la réactiver après les modifications.